NISTIR 8259B

IoT Non-Technical Supporting Capability Core Baseline

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold

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

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

NISTIR 8259B

Internet of Things Non-Technical Supporting Capability Core Baseline

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

Rebecca Herold
The Privacy Professor
Des Moines, IA

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

August 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8259B
21 pages (August 2021)

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

Comments on this publication may be submitted to:

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

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

Non-technical supporting capabilities are actions a manufacturer or third-party organization performs in support of the cybersecurity of an IoT device. This publication defines an Internet of Things (IoT) device manufacturers' *non-technical supporting capability core baseline*, which is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems. The purpose of this publication is to provide organizations a starting point to use in identifying the non-technical supporting capabilities needed in relation to IoT devices they will manufacture, integrate, or acquire. This publication is intended to be used in conjunction with NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline.*

Keywords

cybersecurity baseline; Internet of Things (IoT); securable computing devices.

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 public content, and colleagues at NIST who offered invaluable inputs and feedback. Special thanks to Cybersecurity for IoT team members Brad Hoehn and David Lemire and the NIST FISMA (Federal Information Security Modernization Act) Implementation Project team for their extensive help.

Audience

The main audience for this publication is IoT device manufacturers, especially with the emerging role of product security officers. This publication may also help IoT device customers or integrators.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents, and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Appendices

1 Introduction

Internet of Things (IoT) devices often lack built-in device cybersecurity capabilities, as well as non-technical support relevant to cybersecurity. Customers can use this type of information to help mitigate cybersecurity risks related to the IoT devices and their use. The wide range of connectivity possible for IoT devices, and the ability for these devices to interact with the physical world, means securing these devices often becomes a priority; but it is a challenge for customers when they are not adequately supported.

This publication should be used and understood within the context of NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [1] and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [2]. NISTIR 8259 discusses considerations for manufacturers to help guide them in choosing and implementing the device cybersecurity capabilities their IoT devices will provide. 8259A discusses device technical cybersecurity capabilities, which are cybersecurity features or functions that devices provide through their own technical means (i.e., device hardware and software), and establishes a core baseline of device cybersecurity capabilities IoT device customers commonly need.

To complement the core baseline from NISTIR 8259A, the IoT non-technical supporting capability core baseline is a set of actions performed by manufacturers and/or designated supporting third parties (called *supporting parties*). These actions will help others (e.g., customers, end-users) use the cybersecurity capabilities of IoT devices, and support the on-going cybersecurity of the IoT device and the system and networks the device connects to (the digital ecosystem). Providing such non-technical cybersecurity support through educational materials or other types of non-technical tools and actions can benefit the entire IoT device ecosystem and allow manufacturers to better support the cybersecurity of devices throughout the entire device lifecycle. Both device cybersecurity capabilities and non-technical supporting capabilities are vital to customers' abilities to achieve their needs and goals. Similar to the IoT *device cybersecurity capability* core baseline in NISTIR 8259A, this IoT non-technical supporting capability core baseline is intended to give organizations a starting point for establishing non-technical actions to support IoT device cybersecurity risk management.

Specifically, this publication describes four recommended non-technical supporting capabilities related to the full lifecycle of cybersecurity management that manufacturers should implement to support the IoT devices they make for the full length of life: 1) Documentation; 2) Information and Query Reception; 3) Information Dissemination; and 4) Education and Awareness.

A manufacturer's choice of non-technical supporting capabilities considers the purpose of the IoT device and the intended uses. Such actions make it easier for customers to understand and identify how IoT devices are built to meet their cybersecurity needs as well as the manufacturers' expectations for how the IoT device should be securely used. Figure 1 shows the four non-technical supporting capabilities included in this baseline.

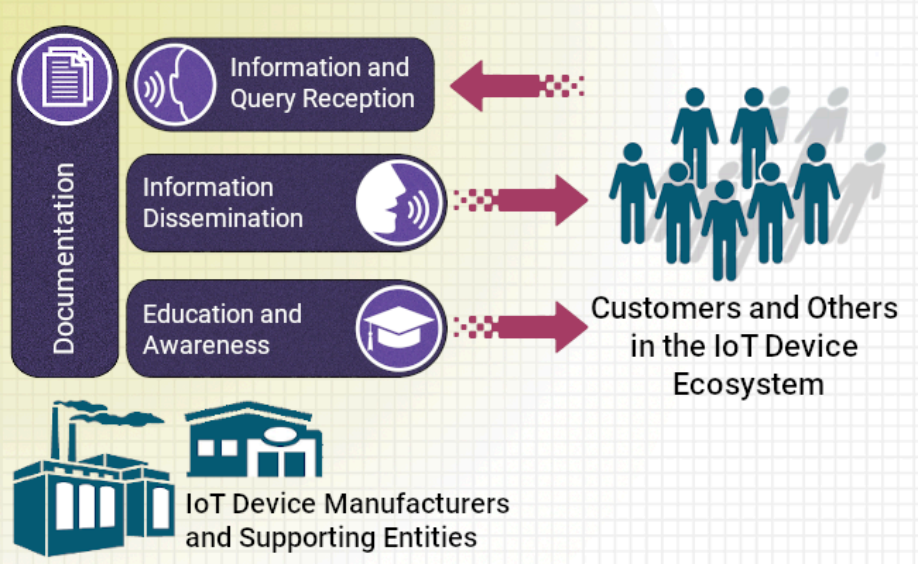

Figure 1: How customers and others in the IoT device ecosystem will use the capabilities in the baseline if provided by IoT device manufacturers and supporting entities.

Documentation captures information potential customers and others in the ecosystem may need to know about the IoT devices and ways in which it, and associated data and systems, can be secured. Such documentation is also often necessary prior to purchase and throughout the IoT device's lifecycle for the customer and others in the ecosystem (e.g., auditors and assessors). This documentation supports the appropriate treatment of risk, compliance, and assurance from internal and external perspectives when the IoT device and associated systems are implemented within the customer environment. As shown in Figure 1, documentation acts as a pillar of support for other non-technical capabilities. This is because other non-technical capabilities, including those in the IoT non-technical supporting baseline, will use the information captured via documentation to customize their delivery.

Information and Query Reception occurs after purchase and allows customers and others in the ecosystem (e.g., researchers, product rating organizations) to submit questions and other information related to securing the IoT device and associated systems. The manufacturer and supporting parties can then respond. Information and query reception can assist customers and others in many ways throughout the lifecycle of an IoT device such as by allowing manufacturers and supporting third -party entities to adapt and update their support services (e.g., provided through other non-technical supporting capabilities) for the customers' cybersecurity needs and goals.

Information Dissemination allows for information to continue to flow to customers and others in the ecosystem about the cybersecurity of their IoT devices and associated systems. Customers and others will benefit from 1) the disclosure of newly discovered cybersecurity vulnerabilities for the device, associated systems and software, etc. and 2) notifications about IoT device

updates, such as software updates, algorithm changes, new protocols, or changes in the vendors used by the manufacturer to update cybersecurity, that may impact cybersecurity risks.[1]

Education and Awareness provides the educational content required to support customers and others in the secure use and safeguarding of IoT devices and associated systems, software, and hardware. By making customers and others in the ecosystem more knowledgeable about how to secure the IoT devices, and how to most effectively use the device's cybersecurity capabilities, manufacturers can help reduce the number of occurrences and related severity of IoT device compromises, thwart attacks against the devices, and reduce the number of vulnerabilities that are exploited and lead to compromised devices.

Customers are the typical recipients of the non-technical supporting capabilities, but some customers may not be able to use these non-technical supporting capabilities directly. In the latter case, the capability might be used by other entities in the IoT device ecosystem (e.g., vendors, trade or professional organizations, advocacy groups, and technology media) to help customers meet their needs and goals.

This baseline was developed after reviewing a variety of guidance documents from multiple sources and receiving input from stakeholders. It represents a coordinated effort to produce a definition of common capabilities not an exhaustive list. The core baseline is intended to be a flexible starting point. Manufacturers and supporting parties can use the IoT non-technical supporting capability core baseline in the context of the activities in NISTIR 8259 and that is appropriate to them. It is important to note that manufacturers and supporting third parties should implement the non-technical supporting capabilities that support the risk management needs of customers of the IoT device within its intended digital ecosystem. This will then result in each of the individual non-technical supporting capabilities in the baseline being implemented in a manner consistent with the needs and expectations of those customers. If additional supporting capabilities are necessary to enable secure use of the devices, organizations are encouraged to consider defining additional supporting capabilities that better suit their use case(s).

[1] One resource supporting both Information Reception and Information Dissemination to others in the ecosystem about vulnerabilities is found in *Draft NIST SP 800-216: Federal Vulnerability Disclosure Guidelines* [17]. This document recommends guidance for establishing a federal vulnerability disclosure framework and highlights the importance of proper handling of vulnerability reports and communicating the minimization or elimination of vulnerabilities.

2 The IoT Non-Technical Supporting Capability Core Baseline

Table 1 defines the IoT device non-technical supporting capability core baseline, which, in combination with the device cybersecurity (technical) capability core baseline of NISTIR 8259A, can make it possible to secure an IoT device. The table below draws from the concepts in Section 4 of NISTIR 8259, which highlights the importance of communication with customers and others in the IoT device ecosystem about cybersecurity, and in Section 3, which provide many examples of information that customers and others may need to know about IoT devices or the design of the device.

Table 1 is a high-level starting point for IoT device manufacturers to understand how they may have to plan for and support the customer's cybersecurity needs and goals in non-technical ways. The complexities of IoT device manufacturing may result in organizations other than the device manufacturer providing critical cybersecurity support such as some or all of the non-technical supporting capabilities described in this publication. Therefore, the target for this guidance includes supporting parties (e.g., cloud service provider and contracted servicer) that may play a role in one or more of the actions in Table 1 in addition to the manufacturer.

The non-technical supporting capabilities in Table 1 describe the intended recipient of the value of the capability as the *customer* (i.e., those with whom the *communications* take place). This stems from an assumption that the customer of an IoT device will have cybersecurity needs, goals, and responsibilities related to the IoT device. For a specific customer or use case, there may be other individuals or entities from the IoT device ecosystem who may be part of that communication. For example, an enterprise customer may have several supporting contractors or entities as well as employees to whom the information described in the table may need to be communicated. Alternatively, a building owner incorporating IoT devices will need to pass information to building tenants using those IoT devices. In this case, it is also noteworthy how future owners/users of the IoT devices (i.e., future tenants) may not be considered *customers* in the traditional sense. Finally, in addition to the customer, for some sectors, there may be robust third-party ecosystem entities (e.g., product reviewers and assessors, retailers, and vendors) that may use non-technical supporting capabilities to help improve the cybersecurity for the sector broadly.

The specific actions listed in the table are meant to reflect the typical actions many customers and others in the IoT device ecosystem expect manufacturers and supporting parties to take to support cybersecurity needs and goals. Manufacturers can choose and customize non-technical capabilities based upon the intended use cases and customers of the IoT device, with examples and rationales provided to give additional information about customer expectations or why these actions are important. As with NISTIR 8259A, more context would be needed to articulate specific non-technical supporting capabilities. Other types of non-technical supporting capabilities may be needed to best address the system context within which the IoT device is used and also in consideration of each IoT device user

organization's[2] system cybersecurity risks. Organizations that choose to adopt the core baseline non-technical capabilities for any of the IoT devices they produce, integrate, or acquire have considerable flexibility in identifying the actions to implement those capabilities that can most effectively address IoT device usage within the customers' own system and their goals and purpose for using IoT devices.

Each row in Table 1 covers one of the device non-technical supporting capabilities in the IoT non-technical supporting capability core baseline:

- The first column describes the non-technical supporting capability.
- The second column provides a numbered list of common actions within that supporting capability. These are actions that an organization implementing the non-technical supporting capability often (but not always) would use to achieve the capability. It is important to understand that the actions are not intended to be comprehensive nor are they presented in any particular order.[3]
- The third column explains the rationale for needing the non-technical support capability.
- The last column lists IoT reference examples that indicate existing sources of IoT device cybersecurity guidance specifying a similar or related capability. Because the table only covers the basics of the capabilities, the references can be invaluable for understanding each capability in more detail and learning how to implement each capability in a reasonable manner. The following are the references used in Table 1:
  - **AGELIGHT**: AgeLight Digital Trust Advisory Group, "IoT Safety Architecture & Risk Toolkit v4.0" [7]
  - **CTA**: Consumer Technology Association, "American National Standards Institute (ANSI)/CTA Standard - Baseline Cybersecurity Standard for Devices and Device Systems: ANSI/CTA-2088" [8]
  - **CSDE**: Council to Secure the Digital Economy (CSDE), "The C2 Consensus on IoT Device Security Baseline Capabilities" [9]
  - **ETSI**: European Telecommunications Standards Institute, "Cyber Security for Consumer Internet of Things: Baseline Requirements v2.1.0" [10]
  - **IoTSF**: IoT Security Foundation (IoTSF), "IoT Security Compliance Framework v2.1" [11]

[2] Note that the "user organizations" could be different from the "customer organization." For example, a connected HVAC system may be purchased by the building owner (customer organization) but used by the building tenants (users).

[3] These common actions often mention typical data involved; however, the specific data elements involved in many of these actions can vary widely due to the range of IoT devices available.

Table 1: Non-Technical Supporting Capabilities

Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Documentation: The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle.	1. Document assumptions made during the development process and other expectations related to the IoT device, such as: a. Expected customers and use cases b. Physical use and characteristics c. Network access and requirements (e.g., bandwidth requirements) d. Data created and handled by the device e. Expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.) f. Assumed cybersecurity requirements for the IoT device g. Laws and regulations with which the IoT device and related support activities comply h. Expected lifespan, anticipated cybersecurity costs related to the IoT device (e.g., price of maintenance), and term of support 2. Document the **device cybersecurity capabilities**, such as those detailed within NISTIR 8259A, that are implemented within the IoT device and how to configure and use them. 3. Document device design and support considerations related to the IoT device, such as:[4] a. IoT platform[5] used in the development and operation of the IoT device and related documentation b. Protection of software and hardware components of the IoT device (e.g., secure boot, hardware root of trust, and secure enclave) c. Consideration of the known risks related to the IoT device and known potential misuses d. Secure software development and supply chain practices used e. Accreditation, certification, and/or evaluation results for cybersecurity-related practices	• This capability supports Information Dissemination and Education and Awareness. • Manufacturers and/or supporting entities should consider documentation throughout their development lifecycle in order to capture cybersecurity-relevant information when it is available so as to ensure access to this information when it is needed. Documentation will begin as internal resources for a manufacturer and/or supporting entity that can be used in various ways. • Documentation of cybersecurity information is foundational to the risk assessment that a manufacturer should preform (as discussed in NISTIR 8259). • Documentation of cybersecurity information can be provided to support potential IoT device customers in making purchase decisions. Customer organizations can require such documentation to ensure that the IoT device will support all the cybersecurity requirements of the customer organization. • Documentation provides an important source of cybersecurity information that helps enable secure use of the IoT device by customers. • Documentation may also be important for audits, accreditations, or other certifications. • Documentation about maintenance requirements, especially regarding the supporting parties the manufacturer contracted by the manufacturer and vendor to perform maintenance, device changes, etc., supports the manufacturer, supporting entity, and/or customers' need to adequately plan for maintenance activities.	• **AGELIGHT**: 11, 12 • **ETSI**: Provision 4.1 • **IoTSF**: 2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.3.7, 2.4.12.5 • **CSDE**: 5.2.3

Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Documentation (*continued*)	4. Document *maintenance* requirements for the IoT device, such as: a. Cybersecurity maintenance expectations and associated instructions or procedures for the customer (e.g., account management, local and/or remote maintenance activities, and vulnerability/patch management plan) b. When maintenance will be performed by supporting parties that will need access (remote or onsite) to customer's IoT devices and their information security contract requirements c. Cybersecurity considerations of the maintenance process (e.g., how does customer data unrelated to the maintenance process remain confidential even to maintainers)	• Documentation of cybersecurity information enables better understanding of the potential risks related to the IoT device, which can inform customers and others in the IoT device ecosystem and guide on-going risk mitigation support. • Documentation helps personnel with the responsibility of securing IoT devices within the system understand the implementation and operation of controls and prevent misuse and compromise by unauthorized entities. • Documentation may be used to supply information about and support the management of supply chain risk, incident response, and other critical cybersecurity functions.	*(see above)*

[4] While this information would be provided by a Software Bill of Materials (SBOM), what is being discussed here is significantly less than what is normally meant by an SBOM. More details on SBOM can be found at https://www.ntia.gov/SBOM.

[5] An IoT platform is typically a third-party vendor provided/hosted SaaS-based tool that is used to support IoT device and endpoint management, connectivity and network management, data management, processing and analysis, application development, cybersecurity, access control, monitoring, event processing, and interfacing/integration. Documentation about such a third party can provide important information about supply chain cybersecurity practices and vulnerabilities to allow for the IoT user to more accurately determine risks related to the use of an IoT platform.

Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive information and queries from the customer and others related to cybersecurity of the IoT device.	1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from their customers and others in the IoT device ecosystem 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support).	• This capability provides input from customers and others in the IoT device ecosystem for the manufacturer to use in the Information Dissemination and Education and Awareness non-technical supporting capabilities. • Customers and others in the IoT device ecosystem may want, or be required, to report vulnerabilities they identify in an IoT device. • Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device. • Some customers may need additional support to securely provision and use an IoT device. • Supports the customers' responsibilities related to cybersecurity, such as enabling them to obtain specialized cybersecurity information that may be used proactively for cybersecurity (e.g., threat intelligence and mitigation, digital forensics investigations, and secure reprovisioning and disposal).	• **CTA**: VUL-002, VUL-003 • **AGELIGHT**: 9 • **ETSI**: Provision 5.2-1 • **IoTSF**: 2.4.3.11, 2.4.3.12 • **CSDE**: 5.2.1, 5.2.2

Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information Dissemination: The ability for the manufacturer and/or supporting entity to broadcast and distribute (e.g., to the customer or others in the IoT device ecosystem) information related to cybersecurity of the IoT device.	1. The procedures to support the ability for the manufacturer and/or supporting entity to alert customers of the IoT device and others about cybersecurity relevant information such as: a. Applicable documentation captured during the design and development of the IoT device b. Software update terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates c. End of term of support or functionality for the IoT device d. Needed maintenance operations e. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability f. An overview of the information security practices and safeguards used by the manufacturer and/or supporting entity g. Accreditation, certification, and/or evaluation results for the manufacturer and/or supporting entity's cybersecurity-related practices h. A risk assessment report or summary for the manufacturer's business environment risk posture 2. The procedures to support the ability for the manufacturer and/or supporting entity to notify customers of cybersecurity-related events and information related to an IoT device throughout the support lifecycle, such as: a. New IoT device vulnerabilities, associated details, and mitigation actions b. Breach discovery related to an IoT device used by the customers and explanations of how to make any associated fixes or actions to prevent similar breaches of other devices.	• This capability supports on-going cybersecurity of the device by keeping customers informed of developments and new information and configuration capabilities after the initial documentation was developed and provided. Information dissemination enables the support, administration, and maintenance necessary to ensure effective and efficient IoT device and system performance and cybersecurity. • Customer organizations may need to be informed about cybersecurity-related activities on the IoT device, such as software updates, algorithm changes, new protocols, or changes in the vendors used by the manufacturer to update cybersecurity, especially if the IoT device is critical to their operations. • Customer organizations will want to stay informed about the cybersecurity of IoT devices to allow them to fine tune their mitigations and maintain an adequate level of risk assurance. • Customer organizations may need to know the cybersecurity practices of the manufacturer and/or supporting entities that have made or will have occasional or ongoing access to the IoT devices to enable them to ensure the other parties do not unacceptably add to the customer's cybersecurity risk. • Customer organizations can use this information to gather insight about the commitment the manufacturer has to information security and to determine the level of risk considered by the manufacturer related to the device. • Customer organizations can view cybersecurity certifications, accreditations, and evaluations for what is typically third-party assurance of acceptable information describing cyber, networking, applications, and related cybersecurity practices.	• **CTA**: REP-005 EoL/EoS-001, EoL/EoS-002, DIN-001, DIN-002 • **AGELIGHT**: 1, 4, 20, 21, 22, 23, 32, 36 • **ETSI**: Provisions 5.3-11, 5.3-12, 5.3-13, 5.3-14, 5.3-16 • **IoTSF**: 2.4.3.9, 2.4.3.14, 2.4.5.35, 2.4.5.36 • **CSDE**: 5.2.3

Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Education and Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity-related information, considerations, features, etc. of the IoT device.	1. Educate customers of the IoT device and others in the ecosystem about the presence and use of device cybersecurity capabilities. For example, it may be important to educate customers and others about: a. How to use *device identifiers* b. How to change configuration settings c. How to configure and use access control functionality d. How to use software update functionality, including aspects such as update validation and/or rollback that may be part of the device cybersecurity capability. 2. Educate customers and others about how an IoT device can be securely reprovisioned or disposed of. 3. Make customers and others aware of their cybersecurity responsibilities related to the IoT device and how responsibilities may be shared between them and others, such as the IoT device manufacturer. (e.g., related to maintenance of the IoT device) 4. Make customers and others aware of key assumptions and expectations related to the cybersecurity of the IoT device that were documented, throughout the full lifecycle of use of the IoT devices, taking into consideration the purpose of the IoT device and the intended uses. Such assumptions should include key dependencies of the IoT device that impact cybersecurity (e.g., connectivity requirements and use of third-party services when in operation). 5. Educate customers and others about how to back-up the data collected from or derived by the IoT device and how to access such data that is stored in cloud storage or other repositories. 6. Educate customers and others about vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT device or associated system that could be used by customers.	• This capability supports secure provisioning and on-going cybersecurity support. • For IoT devices with a wide range of use cases, some customers may need more education than others to securely provision and use an IoT device. • The complexities of IoT systems, devices, and use cases means it is important for manufacturers to create awareness and educate customers and others about cybersecurity of their IoT devices. • Existing regulations and laws require manufacturer and/or supporting entities to provide customers access to the data that manufacturer and/or supporting entities possess about them and also to make such data portable so that customers can take that data and use it elsewhere. • Training reinforced by occasional, ongoing awareness communications. Training examples include providing: • cybersecurity awareness, • instruction in the use of cybersecurity capabilities, and • understanding of cybersecurity-relevant responsibilities supports. Training can result in more secure use of the IoT device and associated systems and prevent mistakes/errors that could result in cybersecurity incidents. Effective training can also reduce the number of vulnerabilities that are exploited and lead to compromised devices.	• **AGELIGHT**: 20, 21, 22, 23, 32, 34, 36 • **ETSI**: Provisions 5.2-1, 5.11-3, 5.12-2, 5.12-3, 6-1, 6-5 • **IoTSF**: 2.4.12.9, 2.4.12.10, 2.4.12.11, 2.4.12.12 • **CSDE**: 5.2.3

References

[1] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[2] Fagan M, 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

[3] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (2018) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[4] Fagan M, Megas, KN, Marron, J, Brady KG, Jr, Cuthill BB, Herold R (2020) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C. https://doi.org/10.6028/NIST.IR.8259C-draft

[5] National Institute of Standards and Technology (2020) IoT Device Cybersecurity Requirement Catalogs. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://github.com/usnistgov/IoT-Device-Cybersecurity-Requirement-Catalogs.

[6] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[7] AgeLight Digital Trust Advisory Group (2020) IoT Safety Architecture & Risk Toolkit v4.0. Updated February 24, 2020. Available at https://www.agelight.com/iot

[8] Consumer Technology Association (2020) *ANSI/CTA-2088 - Baseline Cybersecurity Standard for Devices and Device Systems* (Consumer Technology Association, Arlington, VA). Available at https://csde.org/projects/c2-consensus/

[9] Council to Secure the Digital Economy (2019) The C2 Consensus on IoT Device Security Baseline Capabilities. Available at https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[10] European Telecommunications Standards Institute (2020) *ETSI EN 303 645 v2.1.0 - Cyber Security for Consumer Internet of Things: Baseline Requirements* (European Telecommunications Standards Institute, Valbonne, France). Available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[11] IoT Security Foundation (2020) *IoT Security Compliance Framework v2.1*. (Internet of Things Security Foundation, Livingston, UK). Available at https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/

[12] 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

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

[14] 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

[15] 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

[16] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[17] Schaffer K, Mell P, Trinh H. (2021) Recommendations for Federal Vulnerability Disclosure Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-216. https://doi.org/10.6028/NIST.SP.800-216-draft

Appendix A—Acronyms

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

ACD	Applied Cybersecurity Division
CNSS	Committee on National Security Systems
FISMA	Federal Information Security Modernization Act
IoT	Internet of Things
ITL	Information Technology Laboratory
IR	Internal Report
MAC	Media Access Control
NIST	National Institute of Standards and Technology
SBOM	Software Bill of Materials
SP	Special Publication

Appendix B—Glossary

Selected terms used in this document are defined below.

Communications	The actions and associated activities that are used to exchange information, provide instructions, give details, etc. In the context of this paper, communications refers to the full range of activities involved with providing information to support the secure use of IoT devices. Communications include using such tools as phone calls, emails, user guides, in-person classes, instruction manuals, webinars, written instructions, videos, quizzes, frequently asked questions (FAQ) documents, and any other type of tool for such information exchanges.
Configuration [7, Adapted]	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. The Device Configuration capability does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.
Core Baseline	A set of technical device capabilities needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems.
Customer [12]	The organization or person that receives a product or service.
Device Cybersecurity Capability	Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).
Device Identifier [10, Adapted]	A context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address).
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.

IoT Platform	An IoT platform is typically a third-party vendor provided/hosted SaaS[6]-based tool that is used to support IoT device and endpoint management, connectivity and network management, data management, processing and analysis, application development, cybersecurity, access control, monitoring, event processing, and interfacing/integration. Documentation about such a third party can provide important information about supply chain cybersecurity practices and vulnerabilities to allow for the IoT user to more accurately determine risks related to the use of an IoT platform.
Maintenance [11]	Any act that either prevents the failure or malfunction of IoT device and supporting equipment or restores its operating capability.
Non-Technical Supporting Capability	Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of an IoT device.
Non-Technical Supporting Capability Core Baseline	The non-technical supporting capability core baseline is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
Software	Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries).
Supporting Parties	Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security.
Term of Support	The length of time for which the device will be supported by the manufacturer or supporting parties for such actions and materials as part replacements, software updates, vulnerability notices, technical support questions, etc.
Training	Teaching people the knowledge and relevant and needed cybersecurity skills and competencies that will enable them to understand how to use and configure the IoT devices to enable them to most securely use the IoT devices.
Update [9]	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.

[6] Software-as-a-Service