# Draft 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-draft

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

# Draft NISTIR 8259B

# IoT 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-draft

December 2020


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 8259B
20 pages (December 2020)

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



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

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 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.

## Note to Reviewers

NIST Cybersecurity for IoT Team has chosen a publication strategy of crafting separate documents to address specific concerns within the IoT cybersecurity ecosystem. These documents are part of a single family across the theme of providing guidance to IoT device manufacturers. Industry encouraged this direction in the comments responding to the issuance of Draft NISTIR 8259. The initial foundation documents in this series are as follows:

- **NISTIR 8259:** *Foundational Cybersecurity Activities for IoT Device Manufacturers*
- **NISTIR 8259A:** *IoT Device Cybersecurity Capability Core Baseline*

The new documents in the series that are being released as drafts for comment provide guidance to IoT device manufacturers complementing the guidance. The three additional documents in the NISTIR 8259 series are:

- ***NISTIR 8259B: IoT Non-technical and Supporting Capability Core Baseline*** – NISTIR 8259B complements the NISTIR 8259A device cybersecurity core baseline by detailing what additional, non-technical support is typically needed from manufacturers. This non-technical baseline makes explicit support capabilities like documentation, training support, etc.
- ***NISTIR 8259C: Creating a Profile of the IoT Core Baseline and Non-Technical Baseline*** – NISTIR 8259C presents a method of profiling the core baseline in NISTIR 8259A and the non-technical baseline in NISTIR 8259B to create a more detailed set of capabilities responding to the concerns of a specific sector, based on some authoritative source such as a standard or other guidance. This is the method used to create the profile meeting the requirements of the federal information system low baseline found in draft NISTIR 8259D.
- ***NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*** – NISTIR 8259D presents the profile defining the capabilities needed from and related to IoT devices to incorporate those devices into a federal information system implementing the low baseline controls of NIST SP 800-53.

In addition to the extensions to NISTIR 8259 listed above, the NIST Cybersecurity for IoT Team is also working on **NIST SP 800-213:** ***IoT Device Cybersecurity Guidance for the Federal Government: An Approach for Establishing IoT Device Cybersecurity Requirements*** which explains from a *customer* organization's (i.e., federal agencies and other organizations) perspective how to determine the technical and non-technical capabilities needed from and related to devices to support the SP 800-53 controls they use on their system and in their organization. SP 800-213 enables federal agencies and other organizations to identify needed capabilities for unique situations and turn those selections into requirements for new IoT devices.

NIST appreciates all comments, concerns and identification of areas needing clarification. Ongoing discussion with the stakeholder community is welcome as we work to improve the cybersecurity of IoT devices. **Community input is specifically sought regarding the mapping of specific reference document content to the items in Table 1, to populate the fourth**

**column, "IoT Reference Examples," to strongly aign the NISTIR 8259B baseline to the existing body of cybersecurity guidance. Table 1 in NISTIR 8259A can be used as a model for these informative reference mappings.**

## 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 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

## 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. Examples of non-technical support include providing information about *software updates*, instructions for *configuration* settings, and supply chain information. 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 a challenge for customers when they are not adequately supported.

This publication describes four recommended, but often overlooked, non-technical supporting capabilities related to cybersecurity that manufacturers should consider implementing to support the IoT devices they make: 1) Documentation; 2) Information and Query Reception; 3) Information Dissemination; and 4) Education and Awareness. Potential customers need to know prior to purchase about the ways in which the IoT device, and associated data and systems, can be secured. This information ("Documentation") will help customers make an informed purchase decision. After purchase, this type of information ("Information Dissemination" and "Education and Awareness"), along with information provided to customers to answer questions about securing the device ("Information and Query Reception"), continues to have an important role in securing the IoT device and meeting customers' cybersecurity needs and goals after purchase. Non-technical supporting capabilities include the actions manufacturers or third parties take in support of initial and on-going security of IoT devices. 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' goals for how the IoT device should be securely used. The non-technical cybersecurity capabilities described can support cybersecurity-related customer efforts. By making customers 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.

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. For more information on how the non-technical supporting capabilities described can be incorporated into a manufacturer's development processes, see Section 4 of NISTIR 8259. Organizations can use the IoT non-technical supporting capability core baseline in the context that is appropriate to them. NISTIR 8259A discusses device cybersecurity capabilities, which are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software), and establishes a core baseline of device cybersecurity capabilities needed by many IoT device customers.

To complement the core baseline from NISTIR 8259A, the IoT non-technical supporting

capability core baseline defined in this publication is a set of actions performed by manufacturers and/or designated supporting third parties (called *supporting parties*) that will help customers use the cybersecurity capabilities of IoT devices and support on-going cybersecurity of the IoT device and the system and networks the device connects to. Providing such non-technical cybersecurity support through educational materials or other types of non-technical tools and actions can benefit IoT device customers, 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. Therefore, it is important to understand that the implementation of all non-technical supporting capabilities is not considered mandatory. The individual non-technical supporting capabilities in the baseline may be implemented in full, in part, or not at all. Understanding customer organizations' needs to support risk management in their unique risk environments which include the IoT device and the system within which it operates is the challenge for manufacturers. Understanding this challenge will help manufacturers understand how they implement the non-technical supporting capabilities to meet customer organizations' needs.

This IoT non-technical supporting capability core baseline is not the only set of non-technical supporting capabilities that exists. It represents a coordinated effort to produce a definition of common capabilities, not an exhaustive list. Therefore, if additional supporting capabilities are necessary to enable secure use of the device, organizations are encouraged to consider defining additional supporting capabilities that better suit their use case(s). For more information on IoT device security and privacy considerations, see NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [3]. For a more comprehensive catalog of non-technical supporting capabilities, see the IoT Device Cybersecurity Requirements Catalogs [4]. Device cybersecurity capabilities and non-technical supporting capabilities can be derived or collected from many sources. These sources should be those most pertinent to the organization and system into which the proposed IoT device will be integrated. NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* [5] provides additional guidance on how other sources can be used to understand possible device cybersecurity capabilities and non-technical supporting capabilities that may be needed.

# 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 core baseline of NISTIR 8259A can make it possible to secure an IoT device. The table below follows from NISTIR 8259, drawing from the concepts of Section 4, which highlights the importance of communication with customers about cybersecurity, and Section 3, which provides many examples of information that customers 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 of this guidance is both manufacturers and supporting parties (e.g., cloud service provider, contracted servicer) that may play a role in one or more of the actions in Table 1.

The target of non-technical supporting capabilities (i.e., those with whom the *communications* take place) is summarized in Table 1 as the *customer*. 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 who may be part of that communication. For example, an enterprise customer will have several individuals 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.

The specific actions listed in the table are meant to reflect the typical actions many customers expect manufacturers and supporting parties to take around cybersecurity, 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[1] 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 an IoT

[1] 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).

device usage within the customers' own system, along with the goal and purpose for using the IoT device.

Each row in Table 1 covers one of the device non-technical supporting capabilities in the federal 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.[2]
- The third column explains the rationale for needing the non-technical support capability.
- The last column will be used to list IoT reference examples that indicate existing sources of IoT device cybersecurity guidance specifying a similar or related non-technical supporting capability. Because the table only covers the basics of the capabilities, the references can be invaluable for understanding each non-technical supporting capability in more detail and learning how to implement the corresponding action in a reasonable manner using existing standards. **Please Note**: this column is blank for the Public Comment draft as NIST requests the public to submit recommended informative references for the proposed federal profile.

[2] 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.

316

## Table 1: Non-Technical Supporting Capabilities

| Non-Technical Supporting Capability | Common Actions | Rationale | IoT Reference Examples |
|---|---|---|---|
| **Documentation**: The ability for the manufacturer and/or supporting entity to create, gather, and store information relevant to cybersecurity of the IoT device 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:<br>a. Expected customers and use cases<br>b. Physical use and characteristics<br>c. Network access and requirements<br>d. Data created and handled by the device<br>e. Assumed cybersecurity requirements for the IoT device<br>f. Laws and regulations the IoT device and related support activities comply with<br>g. Expected lifespan, anticipated cybersecurity costs related to the IoT device (e.g., price of maintenance), and term of support<br>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.<br>3. Document device design and support considerations related to the IoT device, such as:[3]<br>a. IoT platform[4] used in the development of the IoT device, and related documentation<br>b. Protection of software and hardware components of the IoT device<br>c. Secure software development and supply chain practices used<br>d. Accreditation, certification and/or evaluation results for cybersecurity-related practices<br>4. Document *maintenance* requirements for the device, such as:<br>a. Cybersecurity maintenance expectations and associated instructions or procedures for the customer (e.g., account management, local and/or remote maintenance activities, vulnerability/patch management plan)<br>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 | • This capability supports Information Dissemination and Education and Awareness.<br>• Documentation of cybersecurity information helps potential IoT device customers to make purchase decisions that support their organization's cybersecurity requirements for IoT device and/or systems where IoT devices are used within.<br>• Documentation of important cybersecurity information helps enable secure use of the IoT device by customers since it serves as the source of information to be provided to customers.<br>• Documentation may also be important for audits or other certifications that some customers may require for IoT devices they use.<br>• 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 customer's need to adequately plan for maintenance activities. | • |

| 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 from the customer information and queries 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, bug bounty programs) from their customers and other types of entities<br>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 for the manufacturer to in turn use in the Information Dissemination and Education and Awareness non-technical supporting capability.<br>• Customer organizations and third-parties may want, or be required, to report vulnerabilities they identify in an IoT device.<br>• Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device.<br>• For broadly used IoT devices, some customers may need additional support to securely provision and use an IoT device. | • |

[3] 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.

[4] 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, security, access control, monitoring, event processing and interfacing/integration. Documentation about such a third-party can provide important information about supply chain security practices and vulnerabilities to allow for the IoT user to more accurately determine risks related to the use of an IoT platform.

| | | | |
|---|---|---|---|
| **Information Dissemination**: The ability for the manufacturer and/or supporting entity to broadcast and distribute 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 about cybersecurity relevant information such as:<br>a. Software update availability or application<br>b. End of term of support or functionality for the IoT device<br>c. Needed maintenance operations<br>d. Cybersecurity and vulnerabilities alerts<br>2. The procedures to support informing customers of activities and procedures used by the manufacturer and/or supporting entity to further consider and safeguard the cybersecurity of the device, such as:<br>a. An overview of the information security practices and safeguards used by the manufacturer and/or supporting entity<br>b. A risk assessment report or summary for the manufacturer's business environment risk posture<br>3. 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:<br>a. New IoT device vulnerabilities, associated details and mitigation actions<br>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 after the initial documentation was developed and provided.<br>• Customer organizations may need to be informed about cybersecurity-related activities on the IoT device, especially if the IoT device is critical to their operations.<br>• 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.<br>• Customer organizations may need to know the security 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.<br>• 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.<br>• Customer organizations can view security certifications, accreditations and evaluations for what is typically third-party assurance of acceptable information describing cyber, networking, applications, and related security practices.<br>• Customer organizations can use the associated documentation to support their evaluation of the adequacy of the security provided by the manufacturer and/or supporting entity and related IoT device.<br>• Customer organizations who must ensure IoT devices comply with the associated laws and regulations for which they are covered can | • |

| Non-Technical Supporting Capability | Common Actions | Rationale | IoT Reference Examples |
|---|---|---|---|
| | | use the documentation to support their IoT purchase decisions and risk assessments. | |
| **Education and Awareness**: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers about cybersecurity-related information, considerations, features, etc. of the IoT device. | 1. Educate customers of the IoT device about the presence and use of device cybersecurity capabilities. For example, it may be important to educate customers about:<br>a. How to use *device identifiers*<br>b. How to change configuration settings<br>c. How to configure and use access control functionality<br>d. How to use software update functionality, including aspects such as update validation that may be part of the device cybersecurity capability<br>2. Educate customers about how an IoT device can be securely reprovisioned or disposed of.<br>3. Make customers 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)<br>4. Make customers aware of key assumptions and expectations related to the cybersecurity of the IoT device.<br>5. Educate customers 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.<br>6. Educate customers about vulnerability management options (e.g., 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.<br>• 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.<br>• The complexities of IoT systems, devices, and use cases means it is important for manufacturers to create awareness and educate customers about cybersecurity of their IoT devices.<br>• Growing numbers of regulations and laws require manufacturer and/or supporting entities 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. | • |

317

318

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

[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. 4. https://doi.org/10.6028/NIST.SP.800-30r1

[7] 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

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

[9] 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

[10] 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

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

[12] International Organization for Standardization (ISO) 9000:2015, Quality management systems – Fundamentals and vocabulary, September 2015.

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

320

## Acronyms

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

| | |
|---|---|
| ACD | Applied Cybersecurity Division |
| CNSS | Committee on National Security Systems |
| 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 |

# 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-based tool that is used to support IoT device and endpoint management, connectivity and network management, data management, processing and analysis, application development, security, access control, monitoring, event processing and interfacing/integration. Documentation about such a third-party can provide important information about supply chain security 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 security skills and competencies by 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. |

335