NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

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

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

NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

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

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew Smith
Huntington Ingalls Industries
Annapolis Junction, MD

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

May 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 8259A
23 pages (May 2020)

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

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

Device cybersecurity capabilities are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software). This publication defines an Internet of Things (IoT) device cybersecurity capability core baseline, which is a set of device capabilities generally needed 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 device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire. This publication can be used in conjunction with NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*.

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 essay and the public comment drafts; and colleagues at NIST who offered invaluable inputs and feedback. Special thanks to Cybersecurity for IoT Program team members Barbara Cuthill and Jeff Marron and the NIST FISMA Implementation Project team for their extensive help in copy editing.

Audience

The main audience for this publication is IoT device manufacturers. This publication may also help IoT device customers or integrators.

Table of Contents

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.

1 Introduction

Computing devices that integrate physical and/or sensing capabilities and network interface capabilities are being designed, developed, and deployed at an ever-increasing pace. These devices are fulfilling customer needs in all sectors of the economy. Many of these computing devices are connected to the internet. A novel characteristic of these devices is the combination of connectivity and the ability to sense and/or affect the physical world. As devices become smaller and more complex, with an increasing number of features, the security of those devices also becomes more complex. This publication defines a baseline set of device cybersecurity capabilities that organizations should consider when confronting the challenge of the Internet of Things (IoT).

Device cybersecurity capabilities are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software). The IoT device cybersecurity capability core baseline (*core baseline*)[1] defined in this publication is a set of device capabilities generally needed to support commonly used cybersecurity controls that protect devices as well as device data, systems, and ecosystems. The concept of a baseline in any context requires careful consideration; security capabilities for IoT devices are no exception.

The core baseline has been derived from researching common cybersecurity risk management approaches and commonly used capabilities for addressing cybersecurity risks to IoT devices, which were refined and validated using a collaborative public-private process to incorporate all viewpoints. Multiple requests for comment were issued, and multiple workshops and roundtables were held. NIST is committed to an open and transparent process that facilitates stakeholder feedback and iterative improvement.

These capabilities were developed in the context of NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [2], which discusses considerations for manufacturers to help guide them in choosing and implementing the device cybersecurity capabilities their IoT devices will provide. NISTIR 8259 also defines terminology and concepts that provide critical context for understanding device cybersecurity capabilities as one part of the entire IoT cybersecurity ecosystem. Thus, though both NISTIR 8259 and this publication have manufacturers as the intended audience, the considerations and capabilities discussed across the two publications can be used by manufacturers, integrators, or consumers. For more information on how these capabilities can be incorporated into a manufacturer's development processes, see NISTIR 8259. Other organizations can use the core baseline in the context that is available and appropriate to them.

Regardless of an organization's role, this baseline is intended to give all organizations a starting point for IoT device cybersecurity risk management, but the implementation of all capabilities is not considered mandatory. The individual capabilities in the baseline may be implemented in

[1] The usage of the term "baseline" in this publication should not be confused with the low-, moderate-, and high-impact system control baselines set forth in NIST Special Publication (SP) 800-53 [1] to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies. In that context, the low-, moderate-, and high-impact control baselines apply to an information system, which may include multiple components, including devices. In this publication, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations, and the *core baseline* described is meant to apply to individual IoT devices.

full, in part, or not at all. It is left to the implementing organization to understand the unique risk context in which it operates and what is appropriate for its given circumstance. For more information on how to conduct a risk assessment, see NIST Special Publication 800-30, *Guide for Conducting Risk Assessments* [3].

Furthermore, this baseline is not the only set of capabilities that exist. This baseline represents a coordinated effort to produce a definition of common capabilities, not an exhaustive list. Therefore, an implementing organization may define capabilities that better suit their organization. Using these additional capabilities to support IoT device cybersecurity risk management is encouraged. For more information on IoT device security and privacy considerations, see NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [4].

2 IoT Device Cybersecurity Capability Core Baseline Definition

Table 1 defines the IoT device cybersecurity capability core baseline. The core baseline's role is as a default for minimally securable devices. However, device cybersecurity capabilities will often need to be added or removed from an IoT device's design, integration, or acquisition to best address an organization's common cybersecurity risks. The core baseline does not specify how the device cybersecurity capabilities are to be achieved, so organizations who choose to adopt the core baseline for any of the IoT devices they produce, integrate, or acquire have considerable flexibility in implementing it to effectively address needs.

Each row in Table 1 covers one of the device cybersecurity capabilities in the core baseline:

- The first column defines the capability. Note that Figure 1, which is located in Appendix A, indicates how the capability relates to the risk mitigation areas and challenges defined in NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [3].
- The second column provides a numbered list of *common elements* of that capability—elements an organization seeking to implement the core baseline often (but not always) would use in order to achieve the capability. (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 capability and its common elements to be included in the core baseline.
- 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 (IoTSA) v3.1" [5]
  - **BITAG**: Broadband Internet Technical Advisory Group (BITAG), "Internet of Things (IoT) Security and Privacy Recommendations" [6]
  - **CSA**: Cloud Security Alliance (CSA) IoT Working Group, "Identity and Access Management for the Internet of Things" [7]
  - **CSDE**: Council to Secure the Digital Economy (CSDE), "The C2 Consensus on IoT Device Security Baseline Capabilities" [8]
  - **CTIA**: CTIA, "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1" [9]

- **ENISA**: European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [10]
- **ETSI**: European Telecommunications Standards Institute (ETSI), "Cyber Security for Consumer Internet of Things" [11]
- **GSMA**: Groupe Spéciale Mobile Association (GSMA), "GSMA IoT Security Assessment" [12]
- **IEC**: International Electrotechnical Commission (IEC), "IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components" [13]
- **IIC**: Industrial Internet Consortium (IIC), "Industrial Internet of Things Volume G4: Security Framework" [14]
- **IoTSF**: IoT Security Foundation (IoTSF), "IoT Security Compliance Framework, Release 2" [15]
- **ISOC/OTA**: Internet Society/Online Trust Alliance (OTA), "IoT Security & Privacy Trust Framework v2.5" [16]
- **NEMA**: National Electrical Manufacturers Association (NEMA), "Cyber Hygiene Best Practices" [17]
- **OCF**: Open Connectivity Foundation (OCF) "OCF Security Specification Version 2.1.2" [18]
- **PSA**: Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members, "PSA Certified™ Level I Questionnaire, Version 2.0 Beta" [19]

Appendix B provides the definitions for the underlined terms in Table 1.

Table 1: The Device Cybersecurity Capability Core Baseline for Securable IoT Devices

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifier 2. A unique physical identifier at an external or internal location on the device authorized entities can access Note: the physical and logical identifiers may represent the same value, but they do not have to.	• This capability 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. This may require that it be immutable to allow for consistent identification using the identifier. The unique logical identifier may also be used for device authentication, but consideration should be made to select an appropriate identifier for the purpose. • 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. • The capability may also need an additional logical identifier that will not necessarily be unique which is used for more specific purposes such as device intent signaling.	• **CSA:** 1 • **CSDE**: 5.1.1 • **CTIA**: 4.13 • **ENISA**: GP-PS-10 • **GSMA**: CLP13_6.6.2, 6.8.1, 6.20.1 • **IEC**: CR 1.2 • **IIC**: 7.3, 8.5, 11.7, 11.8 • **IoTSF**: 2.4.8.1, 2.4.14.3, 2.4.14.4 • **OCF:** 7.1.1 • **PSA:** C1.4, R2.1

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Device Configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.	1. The ability to change the device's software 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 configuration defined by an authorized entity	• This capability supports vulnerability management, access management, data protection, and incident detection. • An authorized entity may want to alter a device's configuration for a variety of reasons, including cybersecurity, interoperability, privacy, and usability. Without a device configuration capability, an authorized entity cannot customize a device to meet its needs, integrate the device into the authorized entity's environment, etc. • Most cybersecurity capabilities are at least somewhat dependent on the presence of a device configuration capability. • 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 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 • **CSA**: 22 • **ENISA**: GP-TM-06 • **IEC**: CR 7.4, CR 7.6 • **IIC**: 7.3, 7.6, 8.10, 11.5 • **IoTSF**: 2.4.8.17, 2.4.15 • **ISOC/OTA**: 26 • **OCF:** 5.3.3, 8.2, 12, 13.3.1 • **PSA**: C2.3, R6.1, R7.1

Device Cybersecurity Capability	Common Elements	Rationale	IoT 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 demonstrably secure 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 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) 3. Configuration settings for use with the **Device Configuration** capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length	• This capability supports access management, data protection, and incident detection. • Authorized entities (e.g, customers, administrators, users) often want the confidentiality of their data protected so unauthorized entities cannot access their data and misuse it. • Authorized entities 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**: 5, 7, 18, 24, 25, 34 • **BITAG**: 7.2, 7.10 • **CSDE**: 5.1.3, 5.1.4, 5.1.5, 5.1.8, 5.1.10 • **CTIA**: 4.8, 5.14, 5.15 • **ENISA**: GP-OP-04, GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-39, GP-TM-40 • **ETSI**: 4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3 • **GSMA:** CLP13_6.4.1.1, 6.11, 6.12.1.1, 6.19, 7.6.1, 8.10.1.1, 8.11.1 • **IEC**: CR 3.1, CR 3.4, CR 4.1, CR 4.2, CR 4.3 • **IIC**: 7.3, 7.4, 7.6, 7.7, 8.8, 8.11, 8.13, 9.1, 10.4, 11.9 • **IoTSF**: 2.4.6.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.16.1, 2.4.16.2 • **ISOC/OTA**: 2, 17, 33 • **OCF:** 8.2, 11.2.1, 11.3, 14.2.2 • **PSA:** C1.1, C1.4, C2.4, D5.2, R2.2, R2.3, R6.1, R7.1

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those 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 to only authorized entities (e.g., device authentication, user authentication) 3. Configuration settings for use with the **Device Configuration** capability including, but not limited to, 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 capability 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. • Access to interfaces may be partially or completely limited based on the device's state. For example, if a device has not been provisioned with proper network credentials, all access to/from network interfaces would be limited if using a secure on-boarding scheme.	• **AGELIGHT**: 10, 13, 14, 15, 16, 19 • **BITAG**: 7.1, 7.2, 7.3, 7.6 • **CSA:** 2, 4, 20 • **CSDE**: 5.1.2 • **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-25, 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**: CLP13_6.9.1, 6.12.1, 6.20.1, 7.6.1, 8.2.1, 8.4.1 • **IEC**: CR 1.1, CR 1.2, CR 1.5, CR 1.7, CR 1.11, CR 2.1, CR 2.2, CR 2.13, CR 7.7, EDR 2.13 • **IIC**: 7.3, 7.4, 8.3, 8.6, 11.7 • **IoTSF**: 2.4.4.5, 2.4.4.9, 2.4.5.5, 2.4.6.3, 2.4.6.4, 2.4.7, 2.4.8 • **ISOC/OTA**: 3, 12, 13, 14, 15, 16 • **NEMA**: Segmenting Networks, User Management, Hardening Devices • **OCF:** 5.1, 5.2, 10, 12 • **PSA:** C2.3, D2.1, D2.2, D2.3, D2.4, D3.1 D3.3, R3.1, R3.2, R3.3, R4.2, R4.5 R6.1

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Software Update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	1. The ability to update the device's software through remote (e.g., network download) and/or local means (e.g., removable media) 2. The ability to verify and authenticate any update before installing it 3. The ability for authorized entities to roll back updated software to a previous version 4. The ability to restrict updating actions to authorized entities only 5. The ability to enable or disable updating 6. Configuration settings for use with the **Device Configuration** capability including, but not limited to: a. The ability to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations b. The ability to enable or disable notification when an update is available and specify who or what is to be notified	• This capability 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. • Some authorized entities will need automatic update capabilities to meet their cybersecurity goals and needs, while others would prefer or need more direct control over updates and their application. • Some organizations may want a rollback capability in the event that an update inadvertently impacts critical applications or integration with other systems, while other organizations may prefer to eliminate the risk of someone intentionally or inadvertently rolling software back to a vulnerable version.	• **AGELIGHT**: 1, 2, 4 • **BITAG**: 7.1 • **CSDE**: 5.1.9 • **CTIA**: 3.5, 3.6, 4.5, 4.6, 5.5, 5.6 • **ENISA**: GP-TM-05, GP-TM-06, GP-TM-18, GP-TM-19 • **ETSI**: 4.3-1, 4.3-2, 4.3-7 • **GSMA**: 7.5.1 • **IEC**: CR 3.4, EDR 3.10 • **IIC**: 7.3, 11.5.1 • **IoTSF**: 2.4.5.1, 2.4.5.2, 2.4.5.3, 2.4.5.4, 2.4.5.8, 2.4.6.1 • **ISOC/OTA**: 1, 6, 8 • **NEMA**: Updating Devices • **OCF:** 14.5 • **PSA:** C2.1, C2.2, R1.1, R1.2, R6.1

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.	1. The ability to report the device's cybersecurity state 2. The ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state 3. The ability to restrict access to the state indicator so only authorized entities can view it 4. The ability to prevent any entities (authorized or unauthorized) from editing the state except for those entities that are responsible for maintaining the device's state information 5. The ability to make the state information available to a service on another device, such as an event/state log server	• This capability supports vulnerability management and incident detection. • Cybersecurity state awareness helps enable investigating compromises, identifying misuse, and troubleshooting certain operational problems. • How the device makes other entities aware of a cybersecurity state will vary based on context-specific needs and goals, but may include capturing and logging information about events in a persistent record that may have to be stored off the device, sending signals to a monitoring system to be handled externally, or alerting via an interface on the IoT device itself.	• **CSDE**: 5.1.7 • **CTIA**: 4.7, 4.12, 5.7, 5.16 • **ENISA**: GP-TM-55, GP-TM-56 • **ETSI**: 4.7-2, 4.10-1 • **GSMA**: CLP13_6.13.1, 7.2.1, 9.1.1.2 • **IEC**: CR 2.8, CR 3.9, CR 6.1, CR 6.2 • **IIC**: 7.3, 7.5, 7.7, 8.9, 10.3, 10.4 • **IoTSF**: 2.4.7.5 • **NEMA**: Monitoring Devices and Systems • **OCF:** 5.1, 5.7, 8.6, 12, 13.8, 13.16 • **PSA**: C1.3, D1.1, D3.2, D3.4, D3.5, D5.1, R4.1, R4.3, R4.4

References

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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/

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

[9] 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/

[10] 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

[11] European Telecommunications Standards Institute (ETSI) (2019) Cyber Security for Consumer Internet of Things. ETSI Technical Specification 103 645 V1.1.1.[2] (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

[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] International Electrotechnical Commission (IEC) (2019) IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components. (International Electrotechnical Commission [IEC], Geneva, Switzerland). https://webstore.iec.ch/publication/34421

[14] 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

[15] IoT Security Foundation (IoTSF) (2018) IoT Security Compliance Framework, Release 2. (IoT Security Foundation [IoTSF], Livingston, Scotland). https://www.iotsecurityfoundation.org/best-practice-guidelines/

[16] Online Trust Alliance (OTA) (2017) IoT Security & Privacy Trust Framework v2.5. (Online Trust Alliance [OTA], an Internet Society initiative). https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

[17] National Electrical Manufacturers Association (NEMA) (2018) Cyber Hygiene Best Practices. (National Electrical Manufacturers Association [NEMA], Rosslyn, VA). https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx

[18] Open Connectivity Foundation (OCF) (2020) OCF Security Specification Version 2.1.2. (Open Connectivity Foundation [OCF], Beaverton, Oregon). https://openconnectivity.org/specs/OCF_Security_Specification_v2.1.2.pdf

[19] Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members (2020) PSA Certified™ Level 1 Questionnaire, Version 2.0 Beta. (Arm Limited, Cambridge, United Kingdom). https://www.psacertified.org/security-certification/psa-certified-level-1

[20] 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

[21] 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

[2] ETSI is currently developing ETSI European Standard 303 645, which is similar to but not identical to the 103 645 Technical Specification cited here. The 303 645 version is not used in this publication because it is still a draft.

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

[23] 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

Appendix A—Understanding the IoT Device Cybersecurity Capability Core Baseline in the Context of Customer Needs and Goals

Organizations should keep in mind that the capabilities presented in Table 1 are meant as a starting point to help provide the means stakeholders may need to meet common cybersecurity needs and goals. Risk mitigation areas that customers may pursue is one way to consider cybersecurity needs and goals that may need to be supported by an IoT device through device cybersecurity capabilities. For example, Figure 1 shows the risk mitigation areas and challenges defined in NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [3] that would be supported, in part, by the capabilities defined in Table 1. NISTIR 8228 cites additional challenges that the core device cybersecurity capabilities do not address because those challenges generally apply to relatively few IoT devices compared to the applicability of the core capabilities.

Figure 1: NISTIR 8228 Risk Mitigation Areas Supported by Each Core Device Cybersecurity Capability

Figure 1 demonstrates that a broad and common set of risk mitigation areas was considered for the core baseline, which should be understood by manufacturers and other readers using the core baseline as a starting point. Though IoT devices providing the basic device cybersecurity capabilities described in the core baseline may help many customers more easily meet their cybersecurity needs and goals while using IoT devices, in reality, customers will likely target different and more specific risk mitigation areas. Therefore, the six capabilities and common elements in Table 1 should not be considered the universal and complete definition of necessary device cybersecurity capabilities for all customers.

As described in NISTIR 8259, manufacturers should consider their IoT device's expected customers and expected use cases to begin to identify the precise device cybersecurity capabilities needed in context. Manufacturers can further define the device cybersecurity capabilities with new or additional elements based on their knowledge and research of their customers. This may mean incorporating device cybersecurity capabilities to support risk mitigations in other areas than what is discussed here (e.g., penetration or other forms of component testing/validation, specific network architectures to reduce risk) or incorporating more unique elements for an IoT device that support less broadly applicable, but in the context of

a customer or use case vitally important risk mitigations and other cybersecurity needs and goals. Manufacturers should also keep in mind other considerations in addition to risk mitigations that may impact device cybersecurity and their elements, such as usability considerations based on the customer and use case, roles and responsibility related to cybersecurity and how customers may expect them to be distributed, and societal cybersecurity needs and goals (e.g., protection against the development of botnets) that may not be directly reflected in the customer's needs and goals, to name a few.

Appendix B—Glossary

Selected terms used in this document are defined below.

Authorized Entity	An entity that has implicitly or explicitly been granted approval to interact with a particular IoT device. The device cybersecurity capabilities in the core baseline do not specify how authorization is implemented for distinguishing authorized and unauthorized entities, but can include identity management and authentication to establish the authorization of entities. It is left to the organization to decide how each device will implement authorization. Also, an entity authorized to interact with an IoT device in one way might not be authorized to interact with the same device in another way.
Configuration	"The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged [20]." 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.
Cybersecurity State	The condition of a device's cybersecurity expressed in a way that is meaningful and useful to authorized entities. For example, a very simple device might express its state in terms of whether or not it is operating as expected, while a complex device might perform cybersecurity logging, check its integrity at boot and report the results, and examine and report additional aspects of its cybersecurity state.
Degraded Cybersecurity State	A cybersecurity state that indicates the device's cybersecurity has been significantly negatively impacted, such as the device being unable to operate as expected, or the integrity of the device's software being violated.
Device Cybersecurity Capability Core Baseline	See *core baseline*.
Device Identifier	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). (This definition is derived from [21].)
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
Interface	A boundary between the IoT device and entities where interactions take place. (This definition is derived from [22].) There are two types of interfaces: network and local.

Local Interface	An interface that can only be accessed physically, such as a port (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) or a removable media drive (e.g., CD/DVD drive, memory card slot).
Logical Identifier	A device identifier that is expressed logically by the device's software. An example is a media access control (MAC) address assigned to a network interface.
Network Interface	An interface that connects the IoT device to a network.
Physical Identifier	A device identifier that is expressed physically by the device (e.g., printed onto a device's housing, displayed on a device's screen).
Software	"Computer programs and associated data that may be dynamically written or modified during the device's execution" (e.g., application code, libraries) [1].
Update	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software. (This definition is derived from [23].)