Draft NISTIR 8259C

Creating a Profile Using the IoT Core Baseline and Non-Technical 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.8259C-draft

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

Draft NISTIR 8259C

Creating a Profile Using the IoT Core Baseline and Non-Technical 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.8259C-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 8259C
25 pages (December 2020)

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

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

Reports on Computer Systems Technology

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

Abstract

The core baseline in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* and the non-technical baseline in NISTIR 8259B, *IoT Manufacturer Non-Technical Supporting Capability Core Baseline* can be expanded upon based on more specific contextual information. Using source material with information pertinent to IoT device *customers'* needs and goals, the central concepts of the NISTIR 8259 series can be used to guide the development of new elaboration on device cybersecurity capabilities an IoT device may need and the non-technical supporting capabilities that may be needed in relation to the IoT device. This process of expanding on the core baseline and non-technical baseline using additional contextual information is called profiling. A process by which readers of the NISTIR 8259 series can profile source documents is described in this publication.

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. 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 collects and 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 800-53B.

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 NIST SP 800-53 controls they use on their system and in their organization. NIST SP 800-213 enables federal agencies 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.

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

List of Figures

1 Introduction

Internet of Things (IoT) devices offer new functionality that can enhance the operations of government, commercial, and other enterprises and provide benefits to consumers and the general public. As such, IoT devices represent a tremendous opportunity for the federal government to leverage scarce resources, but that opportunity comes with new risks, especially in the area of cybersecurity. The NIST Cybersecurity for IoT program has defined IoT devices as "hav[ing] at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long Term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for interfacing with the digital world." [1]

Government, academia and IT companies, both hardware and software, have a decades-long history of researching and developing cybersecurity-related technologies. IoT device manufacturers, especially those newly offering IoT devices or IoT versions of previously existing products, frequently do not have direct experience with that cybersecurity body of knowledge. The NISTIR 8259 series is intended to help bridge that gap for IoT device manufacturers. NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [1] provides guidance to manufacturers on foundational activities to incorporate cybersecurity considerations throughout the product development and lifecycle support process. NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [2] provides a baseline of core cybersecurity device capabilities that are foundational for making IoT devices securable. These technical capabilities have been expanded with non-technical supporting capabilities such as those described within NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [3]. NISTIR 8259B provides a baseline of the non-technical supporting capabilities and actions (for example, documentation, and training) generally needed from manufacturers or other third parties to support common IoT device cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems. The combination of technical and non-technical capabilities as customized for the organization, sector, and/or use case creates what are known as the profiles for the IoT core baseline and non-technical baseline.

This document discusses how to expand on the foundational activities discussed in NISTIR 8259 by providing a process that can be used to create customized profiles (for example, to a specific organization or industry) using the core baseline of cybersecurity device capabilities discussed in NISTIR 8259A and the non-technical baseline discussed in NISTIR 8259B. Specifically, this document expands on activity 3 of NISTIR 8259, "Determine how to address customer needs and goals." The NISTIR 8259A core baseline's six capabilities, and NISTIR 8259B non-technical baseline's four capabilities are a starting point. This document provides a structured process for expanding those baselines to provide all the device cybersecurity capabilities and non-technical supporting actions needed to make the device securable.

Section 2.1 discusses the three concepts central to creating a profile using the core baseline: device-centricity, cybersecurity focus, and minimal securability. Device-centricity is key across the NISTIR 8259 publication series. Unlike many other NIST cybersecurity publications, the NISTIR 8259 series takes a device-centric view because the focus is on the manufacturer of the device and what the manufacturer can do to support cybersecurity goals. Cybersecurity focus is important because there are many other considerations (e.g., privacy, safety, reliability, resilience) which are important but not the focus of this work. Defining a set of technical device capabilities and non-technical supporting capabilities providing minimal device securability depends on what the device is intended to do, what networks the device connects to, and where the device is located. These are critical aspects of the sector use-case used in developing the profile.

Section 2.2 documents the profiling process for the NISTIR 8259 series. This process uses the source documents gathered in the NISTIR 8259 foundational activities of *defining customer use cases* and *gathering relevant source documents* such as relevant regulatory requirements[1], guidance[2] and standards[3]. Critical cybersecurity requirements for those customers are extracted from the relevant source documents. Many new cybersecurity capabilities and supporting non-technical capabilities needed are likely to be sub-capabilities of existing capabilities in the NISTIR 8259 baseline; however, this document also provides a process to document a new top-level capability for a profile.

[1] For example, the US Health Insurance Portability and Accountability Act (HIPAA), the EU General Data Protection Regulation (GDPR), and many others.

[2] For example, guidance from government agencies such as in the US the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Financial Institutions Examination Council (FFIEC), in the EU the National Data Protection Authorities, in Canada the provincial Privacy Commissioners, and in similar roles throughout other countries.

[3] For example, the ISO/IEC 27001 family of standards providing requirements for an information security management system (ISMS). and the CTIA IoT Cybersecurity Certification Program best practices standards.

2 A Process for Creating Profiles Using the IoT Device Cybersecurity Capability and Non-Technical Supporting Capability Baselines

The high-level articulation of cybersecurity device capabilities in the NISTIR 8259A Core Baseline and non-technical supporting capabilities in the NISTIR 8259B Non-Technical Baseline may not provide enough detail to manufacturers when designing IoT devices for specific industry sectors or use cases. It is therefore valuable to *profile* the core baseline for the specific sector or use case. Readers should keep in mind that profiling as defined in this publication can be performed by different entities in the IoT ecosystem, including, but not limited to manufacturers, customers, and trade organizations representing various stakeholders. The goals and perspective of a profile remain the same regardless of the author. The goal of a profile of the core baseline is to take the needs and goals reflected in applicable source documents (e.g., control catalogs, regulatory requirements) and apply the three central concepts to best expand and filter the device cybersecurity requirements for manufacturers.

2.1 Three Central Concepts for Creating a Profile Using the Core Baseline

Cybersecurity is a coordinated goal that places expectations and responsibilities on both device manufacturers and consumers. The NISTIR 8259 series is motivated and scoped to provide guidance for manufacturers that reflects three central concepts: device-centricity, cybersecurity focus, and minimal securability. Each of these three concepts is central to profiling using the core baseline and non-technical baseline.

Device-centricity – Many cybersecurity guidance documents are focused on cybersecurity activities for the system/network and/or organization. For example, NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [4] and the NIST Cybersecurity Framework [5] present controls and outcomes, respectively, that guide organizations to manage cybersecurity risk within a *system* and the larger *organization*. Figure 1 depicts how information systems contain *elements* (including IoT devices) and must conform to and support the technical and organizational security capabilities required to mitigate risks. In addition to the support the system provides for security capabilities, the elements nested within the systems also need to conform to and support the organization's established technical and organizational security capabilities directly.

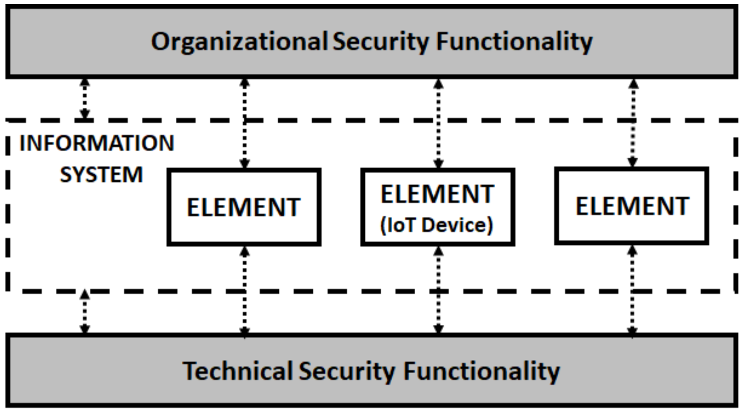

Figure 1 - Information Systems and Associated Elements Support Security Functionality

As organizations acquire an increasing number of diverse IoT devices and these devices become elements of existing systems, the complexity of the cybersecurity challenge increases. The diversity of customer use cases (i.e., how IoT devices will be incorporated into existing systems across a variety of industry sectors) and IoT functionality (i.e., the ways IoT devices can interact with the world) increases the challenges for manufacturers to understand how their IoT devices must support system and organizational security functionality. These concerns have led to a focus on how cybersecurity capabilities at the device level, and supporting capabilities around devices may be required to support system and organizational security functionality. This is called a device-centric view since it scopes cybersecurity capabilities to a connected device, which is often an individual element of a system, rather than an entire system. The device-centric view means that individual IoT devices have cybersecurity capabilities and non-technical supporting capabilities that support system and organizational security functionality[4]. The NISTIR 8259 series takes this device-centric perspective.

Cybersecurity Focus – Cybersecurity is not the only requirement that manufacturers and consumers consider when designing and acquiring IoT devices. Use cases may need to emphasize safety, privacy[5], reliability, or resilience—or other requirements related to the IoT device and its environment of operation—in addition to cybersecurity. Compliance may need to be demonstrated to requirements of these types with varying levels of formality depending on the sector. Cybersecurity must be considered in combination with other prioritized and potentially conflicting requirements in a comprehensive risk management framework.[6] The diversity of use

[4] Note that IT devices also need to have these cybersecurity capabilities and supporting non-technical capabilities, but IT devices have routinely provided these capabilities. Because IoT devices are new and come from manufacturers with a variety of backgrounds with cybersecurity, more explicit definition for this sector is needed.

[5] The NIST Privacy Framework [9] provides more information about privacy needs and goals that may be targeted by customers. Privacy is distinct from cybersecurity, though there are common goals and even capabilities that can help mitigate both cybersecurity and privacy risks.

[6] The five concerns listed (i.e., cybersecurity, privacy, reliability, resiliency, and safety) are used as examples of other considerations or goals beyond cybersecurity from which additional requirements could originate. These five concerns are taken from the NIST Framework for Cyber-Physical Systems [10], where they are identified

cases across IoT devices and industry sectors increases the likelihood that manufacturers must balance the demands of requirements in cybersecurity and in other areas of concern.

Examples of requirements documentation can be found in guidance for devices used in the electric grid addressing reliability, resilience, and human safety [6] and in guidance for medical devices addressing human safety and privacy [7]. Nevertheless, organizations will likely need specific guidance related to device cybersecurity requirements. The NISTIR 8259 series focuses on cybersecurity as the primary goal of the guidance, while considering other concerns where appropriate.

Minimal Securability– NISTIR 8259 defines a *minimally securable* IoT device as one that has "the device cybersecurity capabilities customers may need to mitigate some common cybersecurity risks, thus helping to at least partially achieve their goals and fulfill their needs." This concept of minimal securability is rooted in the idea that manufacturers have an important, but sometimes limited, role in the cybersecurity of an IoT device. The IoT device—as an element of a larger system—must interact with the various other system elements in ways that achieve system security functionality (e.g., through supporting/conforming to security controls). The NISTIR 8259 series also introduces the concept of manufacturer-provided non-technical supporting capabilities. These non-technical capabilities, complementing the technical capabilities, also contribute to a state of minimal securability. The level of support via device cybersecurity and non-technical supporting capabilities needed from an IoT device and/or manufacturer will partially depend on how the customer organization expects to integrate the IoT device within the broader information system. Integration can vary from full integration to minimal integration with the information system. Even minimal integration will require that the IoT device and manufacturer provide minimal support towards cybersecurity. Generally, the more extensive integration requires greater support for cybersecurity.

> In some cases, organizations may want to fully integrate an IoT device with an information system. This would mean the system may require certain cybersecurity capabilities directly from element IoT devices and the organization may require certain non-technical support from manufacturers or third parties. For example, an IoT camera used in an office may require a full network connection and the ability to interact with many other system elements. To minimally secure this camera with the information system, it may need support for various security functionality such as protection of data at rest and in transit, configurable and reliable access control, and vulnerability management just to name a few.
>
> In other cases, organizations may prefer to mitigate risks by configuring the IoT device for use without introducing unacceptable risk (e.g., disable features or aspects of operation), or may prefer to mitigate the risks introduced by the IoT device through additional or compensating controls (e.g., through network segmentation). In these cases, the level of integration and thus support in terms of minimal securability needed from the IoT device and its manufacturer will

---

as the five concerns of the trustworthiness aspect, in the context of that framework, but relate to a hierarchy of considerations that are related, but also sometimes conflicting.

vary and could be low. For example, a small IoT appliance to be used in an office may be placed on a limited sub-network to segment the appliance from other elements of the information system. With the possible risks associated with the IoT device mitigated through network segmentation, there may be little required from the appliance to be considered minimally securable.

Other factors will also influence what constitutes minimal securability for a given IoT device and customer organization, notably how the customer mitigates risk faced by their systems and organization. How risks are mitigated will impact many other aspects of how the IoT device is incorporated into the information system (including the IoT device's level of integration with the information system) and serve as the target of device-centric, cybersecurity-focused guidance produced in profiling.

2.2 Creating a Profile

Understanding the three concepts described above (i.e., device-centricity, cybersecurity focus, and minimal securability) is important to following the process described in this section to create a profile using the core baseline and non-technical baseline. The steps shown in Figure 2 and detailed below explain how a profile can be created using existing source guidance and documents, resulting in a profile that reflects the concepts of device-centricity, cybersecurity focus, and minimal securability and builds upon the IoT device cybersecurity capability core baseline and supporting non-technical baseline.

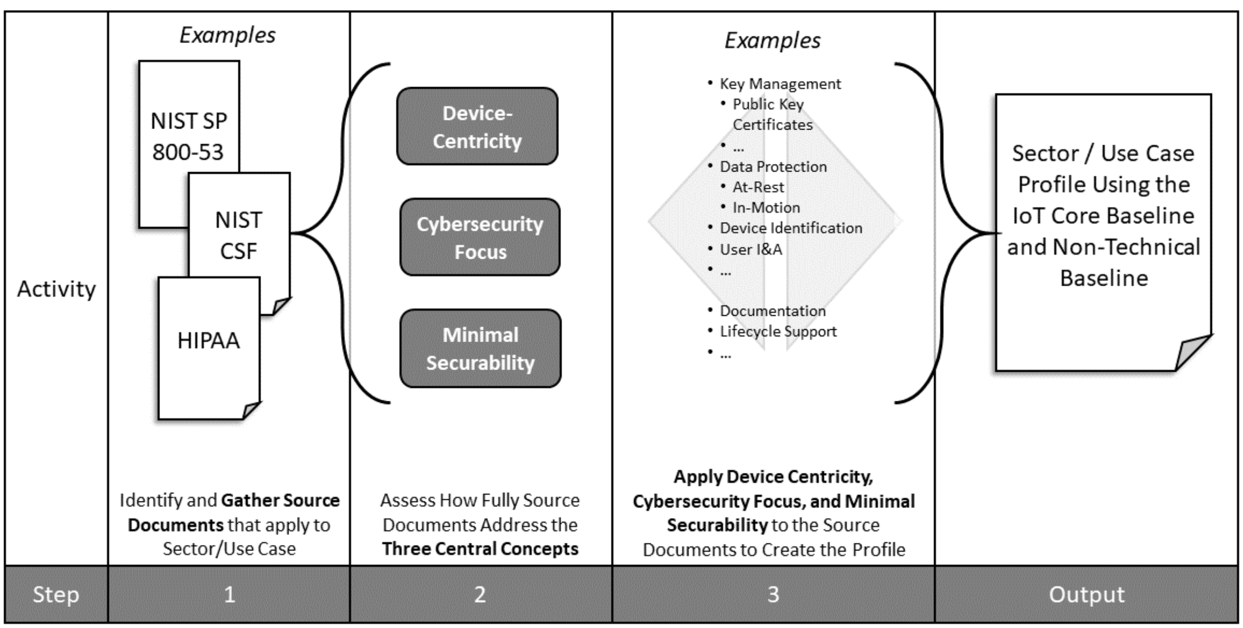

Figure 2 - Three Steps to Creating a Profile Using the Core Baselines

Step 1: Identify and Gather Source Documents for Sector/Use Case Device Cybersecurity Requirements

Source documents are critical to producing a profile of the core baseline and might include controls catalogs, regulatory requirements, guidance documents, contractual requirements, or any other resource important to a particular industry sector or use case. To begin the profiling process, a pertinent set of these source documents must be identified. This document set will serve as the basis for defining customer needs and goals in the sector or use case. This set can reflect common practice in the sector or use case. Thoughtful selection of source documents is vital so that customer cybersecurity needs and goals are adequately represented and understood in the resulting profile.

<u>Different Source Documents Likely for Different Sectors/Use Cases</u>

Each industry sector will likely select different source documents. For example, source documents for the energy sector will likely include the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards and requirements [6]. Whereas, the Healthcare Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule would likely be an appropriate source document when creating a profile for the healthcare industry [7].

Step 2: Assess to What Extent Source Documents Address the Three Central Concepts

With an applicable set of source documents identified, assess whether each source document addresses one or more of the three NISTIR 8259 central concepts (i.e., device centricity, cybersecurity focus, and minimal securability). Some source documents might be device-centric; others might be system or organization-centric. Similarly, source documents might focus exclusively on cybersecurity, but others might focus on privacy, safety, reliability, or resilience (or other concerns). Most common source documents will focus on a combination of these concerns. In some cases, cybersecurity requirements may have to be inferred from requirements around other areas of concerns (e.g., safety, privacy). Unless the source document takes a strict device- and cybersecurity-centric focus with a manufacturer audience in mind, it is unlikely to address minimal securability.

<u>Variability in Need to Apply Central Concepts</u>

Source documents will many times need to have all three concepts applied to create a profile, but it is possible that some will exhibit, in full or in part, one or more of the concepts. For example, some source documents that may be leveraged for cybersecurity, such as requirements from a specific customer or that are a universal minimum for a sector, may already reflect the minimum requirements expected by customers of the IoT device and encapsulate minimal securability. Whereas another source, such as one that describes network-level cybersecurity solutions customers are likely to use, will likely already have a cybersecurity focus, but may lack device-centricity and minimal securability.

Step 3: Apply Device Centricity, Cybersecurity Focus, and Minimal Securability to the Source Documents to Create the Profile

The final step is to work through the needs and goals reflected in the source documents with a focus on applying the concepts of device-centricity, cybersecurity-focus, and minimal securability to identify the applicable device cybersecurity and non-technical supporting capabilities and assemble these into a profile.

To manage any gaps, if multiple source documents are used, it is recommended that source documents be analyzed individually. The analysis of each source document can focus on interpreting applicable device cybersecurity and non-technical supporting capabilities that the customer may need to support the needs and goals from the document while considering any gaps in the central concepts. As discussed in step 2, the selected source documents may have gaps in how they address the concepts of device-centricity, cybersecurity focus, or minimal securability. Where the source already addresses a concept (e.g., cybersecurity focus), consideration of the concept for the purpose of creating a profile may not be necessary. The following describes how each concept can be considered for source documents, as needed:

A. **Device-centricity:** Source documents may describe needs and goals beyond an IoT device, such as solutions and guidance for the network, system, or organizational level. These perspectives will need to be filtered into capabilities an IoT needs *to support* the needs and goals described in the source document. Source documents may represent needs and goals that require both technical and non-technical support for customers. In the context of an IoT device, device cybersecurity capabilities define the technical side and are features and functions provided by the IoT device itself (i.e., through its device hardware and software) in support of cybersecurity needs and goals of customers. These capabilities, when present in an IoT device, can provide technical support for system and organizational security functionality. Non-technical support for IoT devices' cybersecurity is called non-technical supporting capabilities in this publication. These capabilities are actions performed by manufacturers (or possibly their contracted third parties) in support of the securability of a device and can further contribute to minimal securability for some customers. Examples of non-technical capabilities include manufacturer-provided device documentation or online support for a product.

B. Cybersecurity Focus: IoT devices will likely have needs and goals beyond cybersecurity described in source documents (for example, privacy, safety). To create the targeted cybersecurity-focused profile, these other aspects of the source document that describe or address needs and goals other than cybersecurity should be filtered out. Only the cybersecurity related that may impact the device cybersecurity and non-technical supporting capabilities should be identified for the profiling effort.

C. Minimal Securability: Minimal securability is central to the NISTIR 8259 series and profiles created using the core baseline and non-technical baseline should reflect minimal securability. How to define minimal securability will vary by sector and use case. Like any of the three concepts discussed here, in some instances, minimal securability may be reflected in the source document and may not need to be considered directly in the creation of a profile. If this is the case, a profile can be considered complete after the application of the other two central concepts. If not, then the set of device cybersecurity and non-technical supporting capabilities created by application of the other two concepts[7] must be filtered using minimal securability to create a profile. After minimal securability criteria have been applied to the catalog and a subset of capabilities identified, this subset can be considered the profile of the core baseline and non-technical baseline for the sector/use case.

Capabilities developed from each source document should be combined into a coherent catalog. Developing this catalog may require combining closely related capabilities, removing duplicate capabilities, or even organizing capabilities into logical groupings. Checking that catalog against other sources like the NISTIR 8259A core baseline and the NISTIR 8259B non-technical baseline, published sector baselines, or other applicable standards can confirm that all potentially needed device cybersecurity capabilities and supporting non-technical capabilities are included. Appendix A provides a process to work through documenting new capabilities and sub-capabilities. The final set of selected capabilities from this catalog (using the concept of minimal securability as a final filter) organized into a form usable as a requirements definition is the resultant profile.

Structure and Format of Output

Most sectors and use cases will benefit by dividing the profile into at least parts, one for the technical capabilities, and the other for the non-technical supporting actions. This will address the common practice of having different roles for non-technical actions and technical device support. This will allow the two types of roles within the sector or use case to more easily reference the full set of technical or non-technical capabilities that are grouped together. This will also help ensure that the different roles do not leave gaps in the capabilities chosen.

[7] For some sources, this set of capabilities could be considered a *catalog* of device cybersecurity and non-technical supporting capabilities that may have value as an artifact complementary to the profile. This may be a useful tool for instances when customers or manufacturers may desire guidance on capabilities that go beyond the minimal securability reflected in the profile (e.g., when there is flexibility in how specific customers may define their minimal securability).

3 Conclusion

Creating a profile is an essential step in the tailoring of cybersecurity requirements for a specific product to the needs of the specific sector and intended customers of the device. While source documents may be more or less detailed depending on the nature of that sector, the NISTIR 8259A core baseline and NISTIR 8259B non-technical baseline can provide starting points, and this document can provide a structured process for addressing the definition of required cybersecurity device capabilities and non-technical supporting capabilities.

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

[4] 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

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

[6] North American Reliability Corporation (2018) Cybersecurity – Security Management Controls. (North American Electric Reliability Corporation, Washington, DC) Critical Infrastructure Protection Standard CIP-0003-8. Available at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[7] Subrahmanian E, Rachuri S, Bouras A, Fenves SJ, Foufou S, Sriram RD (2006) The Role of Standards in Product Lifecycle Management Support. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7289. https://doi.org/10.6028/NIST.IR.7289

[9] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

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

[11] 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

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

[13] 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

[14] 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

[15] 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

[16] 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 - Creating Sub-Capabilities for Specific Use-Cases and Sectors

The following questions can help guide in the development of new sub-capabilities based on source documents and guidance while profiling. First, you must consider the scope and sources of the new capabilities you are developing (i.e., Step 1) and should consider:

1. For what sector(s) are you developing a profile?
2. What are source documents for cybersecurity goals and needs for customers and use cases in this sector? (e.g., guidance documents, industry standards, regulations, contractual requirements)

To develop a new sub-capability, as described in Step 3, review the format of NISTIR 8259A and NISTIR 8259B, as well as the contents of NISTIR 8259, then consider *commonly necessary*[8] device cybersecurity capabilities and non-technical supporting capabilities to meet or support guidance and requirements in the source documents you identified. You can create sub-capabilities by using the following template:

1. What is the name for the sub-capability (<5 words)?
2. What is a short description of the functionality or actions that comprise the sub-capability (1-2 sentences)?
3. Is this sub-capability technical or non-technical[9]?
    a. Technical
    b. Non-Technical
4. Which capability does this specific sub-capability relate to (select one)?
    a. Device Identity
    b. Device Configuration
    c. Data Protection
    d. Logical Access to Interfaces
    e. Software Update
    f. Cybersecurity State Awareness
    g. Device Security
    h. Documentation
    i. Information and Query Reception (how customers can contact and communicate with the manufacturer or their supporting parties)
    j. Information Dissemination (how manufacturers, or their supporting parties, can provide information to customers)
    k. Education and Awareness
    l. Other?

---

8 Commonly necessary capabilities may not be trivial to identify for all sectors and usually will represent a balance between clear minimal guidance/requirements and flexible, tailorable, additional sector-specific requirements.

9 If you feel the capability is both technical and non-technical, create two capabilities, one with the technical elements and another with the non-technical actions.

5. What are the bulleted abilities (if technical) or actions (if non-technical) of this sub-capability?
6. What are the rationales for this sub-capability and its elements and/or actions?
7. Which sources for cybersecurity goals and needs (or sections/provisions of those source documents) does this sub-capability support?

By documenting and maintaining the answers to the above, the sector or use case will establish a referenceable tool to guide use of the resulting profile and support updates to the profile as the supporting source documents are updated or new ones are created. Such documentation also will likely provide evidence of due diligence and explain to regulators and auditors of entities using the profiles how they made decisions for the implemented abilities and actions.

Appendix B - Acronyms

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

ACD	Applied Cybersecurity Division
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instructions
CSF	Cybersecurity Framework
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
EU	European Union
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information System Modernization Act
GDPR	General Data Protection Regulation
GMT	Greenwich Mean Time
HIPAA	Health Information Portability and Accountability Act
IoT	Internet of Things
ITL	Information Technology Laboratory
IR	Internal Report
LTE	Long Term Evolution
MAC	Media Access Control
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology

PEAP	Protected Extensible Authentication Protocol
RMF	Risk Management Framework
SP	Special Publication
TLS	Transport Layer Security
UHF	Ultra-High Frequency
UTC	Coordinated Universal Time
UWB	Ultra Wide Band
VHF	Very High Frequency

Appendix C - Glossary

Selected terms used in this document are defined below.

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.
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.
Device Cybersecurity Capability	Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).
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 [13, 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).
Interface [14, Adapted]	A boundary between the IoT device and entities where interactions take place. There are two types of interfaces: network and local.
Network Interface	An interface that connects the IoT device to a network.
Non-Technical Baseline	See Non-Technical Supporting Capability Core Baseline

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.
Profile	A profile is a baseline set of minimal cybersecurity requirements for mitigating described threats and vulnerabilities, as well as supporting compliance requirements for a defined scope and type of a particular use case (e.g., industry, information system(s)), using a combination of existing cybersecurity guidance, standards and/or specifications baseline documents or catalogs. A profile organizes selected guidance, standard(s) and/or specification(s) and may narrow, expand and/or otherwise tailor items from the starting material to address the requirements of the profile's target application.
Software [7]	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.
System Element [12]	Member of a set of elements that constitute a system.
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 [7, Adapted]	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.