NIST SPECIAL PUBLICATION 1800-36E

Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management:

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume E:
Risk and Compliance Management

Michael Fagan
Jeffrey Marron
Paul Watrobski
Murugiah Souppaya
National Cybersecurity Center of Excellence
Information Technology Laboratory

Susan Symington
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

William Barker
Dakota Consulting
Largo, Maryland

May 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-36E, Natl. Inst. Stand. Technol. Spec. Publ. 1800-36E, 43 pages, May 2023, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: iot-onboarding@nist.gov.

Public comment period: May 3, 2023 through June 20, 2023

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

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

KEYWORDS

application-layer onboarding; bootstrapping; Internet of Things (IoT); Manufacturer Usage Description (MUD); network-layer onboarding; onboarding; Wi-Fi Easy Connect.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Amogh Guruprasad Deshmukh	Aruba, a Hewlett Packard Enterprise company
Dan Harkins	Aruba, a Hewlett Packard Enterprise company
Danny Jump	Aruba, a Hewlett Packard Enterprise company
Andy Dolan	CableLabs
Kyle Haefner	CableLabs
Craig Pratt	CableLabs
Darshak Thakore	CableLabs
Bart Brinkman	Cisco
Eliot Lear	Cisco
Peter Romness	Cisco
Tyler Baker	Foundries.io
George Grey	Foundries.io
David Griego	Foundries.io
Fabien Gremaud	Kudelski IoT
Brecht Wyseur	Kudelski IoT
Faith Ryan	The MITRE Corporation

Name	Organization
Nicholas Allot	NquiringMinds
Toby Ealden	NquiringMinds
Alois Klink	NquiringMinds
John Manslow	NquiringMinds
Antony McCaigue	NquiringMinds
Alexandru Mereacre	NquiringMinds
Craig Rafter	NquiringMinds
Loic Cavaille	NXP Semiconductors
Mihai Chelalau	NXP Semiconductors
Julien Delplancke	NXP Semiconductors
Anda-Alexandra Dorneanu	NXP Semiconductors
Todd Nuzum	NXP Semiconductors
Nicusor Penisoara	NXP Semiconductors
Laurentiu Tudor	NXP Semiconductors
Michael Richardson	Sandelman Software Works
Mike Dow	Silicon Labs
Steve Egerter	Silicon Labs
Pedro Fuentes	WISeKey

Name	Organization
Gweltas Radenac	WISeKey
Kalvin Yang	WISeKey

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Collaborators		
Aruba, a Hewlett Packard Enterprise company	Kudelski IOT	Sandelman Software Works
CableLabs	NquiringMinds	Silicon Labs
Cisco	NXP Semiconductors	WISeKey
Foundries.io	Open Connectivity Foundation (OCF)	

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

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

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

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

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

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. 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: iot-onboarding@nist.gov.

Contents

List of Tables

1 Introduction

In this project, the National Cybersecurity Center of Excellence (NCCoE) applies standards, recommended practices, and commercially available technology to demonstrate various mechanisms for trusted network-layer onboarding of IoT devices and lifecycle management of those devices. We show how to provision network credentials to IoT devices in a trusted manner and maintain a secure posture throughout the device lifecycle.

This volume of the NIST Cybersecurity Practice Guide discusses the threats and vulnerabilities addressed by the trusted IoT device network-layer onboarding and lifecycle management reference design and maps the reference design's cybersecurity functions to cybersecurity standards and recommended practices. Initial capability mappings are provided from the logical components of the reference design to several cybersecurity standards and recommended practice documents. None of the mappings we provide are intended to be exhaustive; they all focus on the strongest relationships involving each cybersecurity function in order to help organizations prioritize their work. In future drafts of this volume, the NCCoE plans to provide additional mappings from each of the builds that have been implemented as part of this project to those same cybersecurity standards and recommended practices.

1.1 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design for implementing trusted IoT device network-layer onboarding and lifecycle management and describes various example implementations of this reference design. Each of these implementations, which are known as *builds,* is standards-based and is designed to help protect networks by preventing unauthorized devices from connecting to them. These builds are also designed protect IoT devices by preventing them from connecting to unauthorized networks (i.e., impostor networks that may be trying to deceive the device into connecting to them). The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling organizations to incorporate trusted IoT device network-layer onboarding and lifecycle management into their legacy environments according to goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

When complete, this guide will contain five volumes:

- NIST SP 1800-36A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-36B*: Approach, Architecture, and Security Characteristics* – what we built and why

- NIST SP 1800-36C: *How-To Guides* – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project
- NIST SP 1800-36D: *Functional Demonstrations* – use cases that have been defined to showcase trusted IoT device network-layer onboarding and lifecycle management security capabilities and the results of demonstrating these use cases with each of the example implementations
- NIST SP 1800-36E*: Risk and Compliance Management* – risk analysis and mapping of trusted IoT device network-layer onboarding and lifecycle management security functions to cybersecurity standards and recommended practices **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-36A*, which describes the following topics:

- challenges that enterprises face in migrating to the use of trusted IoT device network-layer onboarding
- example solutions built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-36B*, which describes what we did and why.

Also, Section 4 of *NIST SP 1800-36E* will be of particular interest. Section 4, *Mappings*, maps logical components of the reference design to security characteristics listed in various cybersecurity standards and recommended practices documents, including *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) and *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53).

You might share the *Executive Summary, NIST SP 1800-36A*, with your leadership team members to help them understand the importance of using standards-based trusted IoT device network-layer onboarding and lifecycle management implementations.

IT professionals who want to implement similar solutions will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-36C*, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. Also, you can use *Functional Demonstrations, NIST SP 1800-36D*, which provides the use cases that have been defined to showcase trusted IoT device network-layer onboarding and lifecycle management security capabilities and the results of demonstrating these use cases with each of the example implementations.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a trusted IoT device network-layer onboarding and lifecycle management solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and recommended practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated, and additional volumes will also be released for comment. We seek feedback on the publication's contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to iot-onboarding@nist.gov.

2 Risk Assessment

This section discusses the threats and vulnerabilities addressed by the trusted IoT device network-layer onboarding and lifecycle management reference architecture and the residual risk not addressed by it.

2.1 Vulnerabilities

On most home networks, IoT devices are not provided with unique credentials, making home networks vulnerable to having unauthorized devices connect to them if the shared network password falls into the wrong hands, which can happen relatively easily. It also means that networks permit devices to connect to them simply because the device presents the correct shared password, regardless of the device's type or identity, or whether it has any legitimate reason to connect to the network. Also, many IoT devices are manufactured to be as inexpensive as possible, which sometimes means that the devices are not equipped with secure storage, cryptographic modules, unique, authoritative birth credentials, or other features needed to enable the devices to be identified and authenticated. This can make it impossible for a network to determine if a device attempting to connect to it is the intended device. Lack of these features can also make it impossible to protect the confidentiality of a device's network credentials, both during the provisioning process and after the credentials have been installed on the device. Conversely, although it is relatively easy for one network to masquerade as another, IoT devices often do not authenticate the identity of the networks to which they allow themselves to be onboarded and connected, making those devices vulnerable to being taken over and controlled by unauthorized networks.

If devices are manually provisioned with their network credentials, the provisioning process is error-prone, cumbersome, and vulnerable to having the device's network credentials disclosed. If the devices are provisioned automatically over Wi-Fi or some other interface that does not use an encrypted channel, the credentials are also vulnerable to unauthorized disclosure. If the network credentials are not provisioned in a trusted manner, the credentials are vulnerable to disclosure not only the first time the device is onboarded to the network, but every time it is onboarded, which may occur many times during the device lifecycle. For example, the device may need to be re-onboarded periodically to change its credentials in accordance with security policy, or it may need to be re-onboarded due to a security breach, hardware repair, security update, or other reasons. Any insecure features of the onboarding process, therefore, will render the device and network vulnerable every time the device is onboarded.

2.2 Threats

Historically IoT devices have not tended to be onboarded to networks in a trusted manner. This has left networks open to the threat of having unauthorized devices connect to them. Unauthorized devices that are able to connect to a network are able to send and receive data on that network, scan the network for vulnerabilities, eavesdrop on the communications of other devices, and attack other connected devices to exfiltrate or modify their data or to compromise those devices and co-opt them into service to launch distributed denial of service attacks.

Conversely, devices may also be unwittingly tricked into onboarding and connecting to networks that are not authorized to control them. These devices may then be taken control of by those unauthorized networks and thereby prevented from connecting to and providing their intended function on their authorized network.

Even if a device is authorized to connect to a network and the network is authorized to control the device, if the device has not been onboarded in a trusted manner, then other security-related operations that are performed after the device has connected to the network may not have as secure a foundation as they would if the device had been onboarded in a trusted manner. For example, if device intent enforcement is performed but the integrity and confidentiality of the communicated device intent information was not protected (as it would be by a trusted network-layer onboarding mechanism), then trust in the device intent enforcement mechanism may not be as robust as it could have been. Similarly, if application-layer onboarding is performed after the device connects, but the information needed to bootstrap the application-layer onboarding process did not have its integrity and confidentiality protected (as it would be by a trusted network-layer onboarding mechanism), then trust in the application-layer onboarding mechanism may not be as robust as it could have been. Lack of trust in the application-layer onboarding mechanism may, in turn, undermine trust in the device lifecycle management or other application-layer service that is invoked as part of the application-layer onboarding process.

If a device is compromised while in the supply chain or at some other point prior to being onboarded, then even though the device may be onboarded in a trusted manner, it may still pose a threat to the network, its data, and all devices connected to it. If, on the other hand, the trusted network-layer onboarding mechanism is integrated with a device attestation or supply chain management service that is capable of evaluating the integrity of the device and detecting that it has been compromised, the trusted network-layer onboarding mechanism could prevent such a compromised device from being onboarded and connected to the network.

2.3 Risk

Use of trusted network-layer onboarding is designed to enable IoT devices to be provisioned with unique local network credentials in a manner that preserves credential confidentiality. As part of the trusted network-layer onboarding process, the device and the network may mutually authenticate one another, thereby protecting the network from having unauthorized devices connect to it and the device from being taken over by an unauthorized network. However, if the network also enables devices that do not support the trusted network-layer onboarding solution to be provisioned with network credentials and connect to it using a different (untrusted) onboarding solution, the network and all devices on it will still be at risk from IoT devices that have been onboarded using untrusted mechanisms, and the devices that are onboarded using untrusted mechanisms will still be at risk of being taken over by networks that are not authorized to control them.

The trusted network-layer onboarding solution leverages the device's unique, authoritative *birth credentials*, which are provisioned to the device by the device manufacturer and must consist, at a minimum, of a unique device identity and a secret. The trustworthiness of the network-layer onboarding process and the network credentials that it provisions to the device depends on the uniqueness, integrity, and confidentiality of the device's birth credentials which, in many cases, depend on the device's hardware root of trust. If the manufacturer does not ensure that the device's credentials are unique, the identity of the device cannot be definitively authenticated. If the manufacturer is not able to maintain the confidentiality of the secret that is part of the device credentials, the trustworthiness of the device authentication process will be undermined, and the channel over which the device's credentials are provisioned will be vulnerable to eavesdropping.

The trusted network-layer onboarding solution depends upon the trustworthiness of the device's secure storage to ensure the confidentiality of the device and network credentials. If the device's secure storage is vulnerable, the trustworthiness of the network-layer onboarding process and of the confidentiality of the device's network credentials will be compromised. If the secure storage in which the device's network credentials are stored is vulnerable, the network will be at risk of having unauthorized devices attach to it.

If the trusted network-layer onboarding mechanism is integrated with additional security capabilities such as device attestation, device communications intent enforcement, application-layer onboarding, and device lifecycle management, it can further increase trust in both the IoT device and, by extension, the network to which the device connects, assuming that these additional security capabilities themselves are secure and robust. If these security capabilities are not implemented correctly, then integrating with them is of no additional value and in fact may provide a false sense of security.

3 Mapping Use Cases, Approach, and Terminology

The remainder of this volume describes the mappings between cybersecurity functions performed by the reference design's logical components (see NIST SP 1800-36B Section 4) and the security characteristics enumerated in a variety of relevant cybersecurity documents. These mappings are intended for any organization that is interested in implementing trusted IoT device network-layer onboarding and lifecycle management or that has begun or completed an implementation. The mappings provide information on how cybersecurity functions from the reference design are related to:

- *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework—CSF) 1.1 [1] subcategories,
- NIST SP 800-53r5 (*Security and Privacy Controls for Information Systems and Organizations*) [2] security controls,

All of the elements in these mappings—the trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions, CSF Subcategories, and SP 800-53 controls—are concepts involving ways to reduce cybersecurity risk. In future versions of this document, the NCCoE may perform additional mappings between trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions and security characteristics enumerated in other cybersecurity standards, directives, recommended practices, memoranda, etc.

3.1 Use Cases

There are two primary use cases for this mapping. They are not intended to be comprehensive.

1. **Why should organizations implement trusted IoT device network-layer onboarding and lifecycle management?** This use case identifies how implementing trusted IoT device network-layer onboarding and lifecycle management can support organizations with achieving CSF Subcategories and SP 800-53 controls. This helps communicate to an organization's chief information security officer, security team, and senior management that expending resources to implement trusted IoT device network-layer onboarding and lifecycle management can also aid in fulfilling other security requirements.
2. **How can organizations implement trusted IoT device network-layer onboarding and lifecycle management?** This use case identifies how an organization's existing implementations of CSF Subcategories and SP 800-53 controls, can help support a trusted IoT device network-layer onboarding and lifecycle management implementation. An organization wanting to implement trusted IoT device network-layer onboarding and lifecycle management might first assess its current security capabilities so that it can plan how to add missing capabilities and enhance existing capabilities. Organizations can leverage their existing security investments and prioritize future security technology deployment to address the gaps.

3.2 Mapping Producers

The NCCoE trusted IoT device network-layer onboarding and lifecycle management project team performed the initial mapping.

3.3 Mapping Approach

In addition to performing general mappings between the reference design's cybersecurity functions and various sets of security characteristics, the NCCoE intends to also develop mappings that are specific to each trusted IoT device network-layer onboarding and lifecycle management example implementation. To develop these build-specific mappings, the NCCoE intends to ask the collaborators for each build to indicate the mapping between the cybersecurity functions their technology components provide in that build and the sets of security characteristics. These build-specific mappings will appear in future drafts of this document.

Using the logical components in the reference design as the organizing principle for the initial mapping of cybersecurity functions to security characteristics is intended to make it easier for collaborators to map their build-specific technology contributions. Using this approach, the build-specific technology mappings will be instantiations of the project's general reference design mappings for each document.

3.3.1 Mapping Terminology

A *mapping* defines a relationship between two entities. For this mapping, we have used the following relationship types to describe how the functions in our reference design are related to NIST and other reference documents. Note that the *Supports* relationship applies to use case 1 only and the *Is Supported By* relationship applies to use case 2 only.

- **Supports**: trusted IoT device network-layer onboarding and lifecycle management function X *supports* security control/subcategory/capability/requirement Y when X can be applied alone or in combination with one or more other functions to achieve Y in whole or in part.
- **Is Supported By**: trusted IoT device network-layer onboarding and lifecycle management function X *is supported by* security control/subcategory/capability/requirement Y when Y can be applied alone or in combination with one or more other security controls/subcategories/measures to achieve X in whole or in part.
- **Is Equivalent To**: trusted IoT device network-layer onboarding and lifecycle management function X *is equivalent to* security control/subcategory/capability/requirement Y when X is the function that Y describes.

Each *Supports* and *Is Supported By* relationship has one of the following properties assigned to it:

- **Example of**: The supporting concept X is an *example of* how the supported concept Y can be achieved in whole or in part. However, Y could also be achieved without applying X.

- **Integral to**: The supporting concept X is *integral to* the supported concept Y when X must be applied as part of achieving Y.
- **Precedes**: The supporting concept X *precedes* the supported concept Y when X must be achieved before applying Y.

When determining whether a reference design function's support for a given CSF Subcategory or SP 800-53 control is integral to that support versus an example of that support, we do not consider how that function may in general, outside the context of our reference design, be used to support the subcategory, control, capability, or requirement. Rather, we consider only how that function is intended to support that subcategory, control, capability, or other item within the context of our reference design.

Also, when determining whether a function is supported by a CSF subcategory, SP 800-53 control, capability, etc. with the relationship property of *precedes*, we do not consider whether it is possible to apply the function without first achieving the subcategory, control, capability, or other measure. Rather, we consider whether, according to our reference design, the subcategory, control, capability, etc. is to be achieved prior to applying that function.

3.3.2 Mapping Process

The process that the NCCoE used to create the mapping from the logical components of the reference design to the security characteristics of a given document was as follows:

1. Create a table that lists each of the logical components of the reference design in column 1.
2. Describe each logical component's cybersecurity function in column 2.
3. Map each cybersecurity function to each of the security characteristics in the document to which the function is most strongly related and list each of these security characteristics on different sub-rows within column 3. Begin each security characteristic entry with an underlined keyword that describes the mapping's relationship type (i.e., *Supports*, *Is Supported By*, *Is Equivalent To*). After a keyword indicating a relationship type of Supports or Is Supported By, put in parentheses the underlined keyword(s) describing the relationship's property (i.e., *Example of*, *Integral to*, or *Precedes*).
4. In the fourth column, provide a brief explanation of why that relationship type and property apply to the mapping.
5. After completing the mapping table entries as described above for all the logical components in the reference design, examine the mapping in the other direction, i.e., starting with the security characteristics listed in the document and considering whether they have a relationship to the logical components' cybersecurity functions in the reference design. In other words, step

through each of the security characteristics in the document and determine if there is some logical component in the reference design that has a strong relationship to that security characteristic. If so, add an entry for that security characteristic mapping to that logical component's row in the table. By examining the mapping in both directions in this manner, security characteristic mappings are less likely to be overlooked or omitted.

6. Once these steps are complete, any rows in the table that don't have any mappings should be deleted.

The NCCoE applied this mapping process separately for each reference document. None of the mappings are intended to be exhaustive; they all focus on the strongest relationships involving each cybersecurity function in order to help organizations prioritize their work. Mapping every possible relationship, no matter how tenuous, would create so many mappings that it would greatly diminish their value for prioritization.

4 Mappings

The mappings are organized in the remainder of this document as follows:

- Section 4.1 – NIST CSF 1.1 [1]
- Section 4.2 – NIST SP 800-53r5 [2]

In each section, the mapping from the logical components of the reference design is provided first, followed by placeholders for each of the build-specific mappings that we plan to develop for the builds that have been completed so far. Builds are denoted using the names defined in volume B (*Build 1*, *Build 2*, *etc.*). The composition of the builds is described in the appendices of volume B.

4.1 Mapping Between Reference Design Functions and NIST CSF Subcategories

In Table 4-1 we provide a mapping between the logical components of the reference design and the NIST CSF subcategories. This table indicates how trusted IoT device network layer onboarding and lifecycle management functions help support CSF subcategories and vice versa.

Table 4-1 Mapping Between Reference Design Logical Components and NIST CSF Subcategories

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Creates, signs, and installs the device's unique identity and other birth credentials into secure storage. Installs info the device requires for application-layer onboarding (if applicable). Creates a record of devices that it has created.	Supports (example of) ID.AM-1: Physical devices and systems within the organization are inventoried	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, it will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Is Supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The device owner's expectations regarding the capabilities that the device should have (e.g., need for hardware-based secure storage, onboarding-specific firmware and software, and network- and application-layer onboarding credentials) must be clear before the manufacturer creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The manufacturer's factory provisioning process is responsible for generating and providing the device with a unique identity and credential (i.e., birth credential) that can be securely stored and cryptographically authenticated.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner, and it may also be the mechanism for providing device ownership information to the device itself. Device bootstrapping information is information (e.g., a public key that pairs with the device's private key) that the device owner requires to perform trusted network-layer onboarding.	Supports (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Is Supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information from the manufacturer to the device owner must be made clear so the manufacturer will use the expected mechanism (e.g., enrollment of the device's credential into a certificate authority, direct transfer of the bootstrapping information into the device owner's database, or use of a QR code that is imprinted on the device or its packaging).
		Supports (precedes) PR.AC-1: Identities	The generation and transfer of device bootstrapping information from the

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
Network-Layer Onboarding Component	Runs the onboarding protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The network-layer onboarding service is responsible for providing authenticated, authorized devices with a network-layer credential.
		Supports (integral to) PR.AC-3: Remote access is managed	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The network-layer onboarding component is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The network-layer onboarding component authenticates an IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated	The network-layer onboarding component authenticates the IoT device.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		(e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	
		Is Supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The network-layer onboarding component of the device owner must be in possession of the device bootstrapping information in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the device owner must be defined, well-understood, and trusted by both parties.
		Is Supported by (example of) PR.AT-2: Privileged users understand their roles and responsibilities	In some network-layer onboarding protocols, participation of a trusted onboarder is required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network with the device's bootstrapping information. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The network-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Access Point, Router, or Switch	Wireless access point and/or router or switch. The router may get configured with per-device ACLs and role policy when devices are onboarded.	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When a device is onboarded, access control lists (ACLs) and policy for the device may be configured on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	The authorization service provides the network onboarding component and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any special roles or be subject to any specific access controls. The authorization service may also help enable the device to de-	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	termine if the network is authorized to onboard it.		
IoT Device	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the onboarding protocol and interacts with the network onboarding component to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as performing a secure boot process, performing trusted firmware updates, and securely conveying its device intent information.	<u>Supports (integral to)</u> PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		<u>Supports (integral to)</u> PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
Secure Storage	Storage on the IoT device is designed to be protected from unauthorized	<u>Supports (integral to)</u> PR.AC-1: Identities and credentials are issued, managed, veri-	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to ensuring that the

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	access and capable of detecting attempts to hack or modify its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	fied, revoked, and audited for authorized devices, users, and processes	device's identity can be uniquely authenticated.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) PR.DS-1: Data-at-rest is protected	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The fact that a credential is signed by a trusted CA provides a mechanism that may be used for enabling the credential to be verified and revoked.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	If the device credential is an X.509 certificate (e.g., an IDevID) that is signed by a CA, this certificate binds the device's credential to the device's identity.
Application-Layer Onboarding Service	After the device connects to the network, this component interacts with the device using an application-layer onboarding	Is Supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	In some application-layer onboarding mechanisms, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	protocol to authenticate the device, verify that it is authorized to be application-layer onboarded, establish a secure channel with it, and securely provision application-layer credentials to it. The application-layer credentials will allow the device to authenticate to an application-layer service. The application layer service may be a lifecycle management service that can be used to securely and automatically update and patch the device on an ongoing basis.	<u>Supports (example of)</u> ID.AM-2: Software platforms and applications within the organization are inventoried	The process of application-layer onboarding a device may serve as an automatic mechanism to inventory and keep track of which devices have application-related software installed and are therefore capable of interoperating with the application service.
		<u>Supports (integral to)</u> PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
		<u>Supports (integral to)</u> PR.DS-2: Data-in-transit is protected	The application-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
Continuous Authorization Service	Performs a set of ongoing, policy-based assurance and authorization checks on the IoT device to support device lifecycle monitoring and control. For example, it may perform	<u>Supports (example of)</u> ID.RA-3: Threats, both internal and external, are identified and documented	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify potential threats.
		<u>Supports (example of)</u> ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts	The ongoing device authorization service may perform policy-based authorization of devices based on behavioral analyses, device attestation, and other mechanisms.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	behavioral analysis or device attestation and use the results to determine whether the device should be granted access to certain high-value resources, assign the device to a particular network segment, or take other action.	are used to determine risk	
		Supports (example of) ID.RA-6: Risk responses are identified and prioritized	The ongoing device authorization service may quarantine a device, refuse a device access to the network or to certain high-value resources, or take other pre-defined actions based on policy.
		Supports (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity against a baseline to detect anomalies and events.
		Supports (example of) DE.AE-3: Event data are collected and correlated from multiple sources and sensors	The ongoing device authorization service may collect and correlate data from device attestation services, behavioral analytics tools, authentication services, and other sources as input to its policy-based assessment of device authorization.
		Supports (example of) DE.AE-5: Incident alert thresholds are established	If the policy-based assessment of the device does not meet certain policy criteria, the device may not be authorized to access specific resources or the network itself.
		Supports (example of) RS.MI-1: Incidents are contained	If the policy-based assessment of the device does not meet certain policy criteria, and, as a result, the device is denied access to the network or other resources, such restriction may help contain incidents that involve the device.

4.1.1 Mapping between Build 1 and CSF Subcategories

This mapping will be provided in a future version of this document.

4.1.2 Mapping between Build 2 and CSF Subcategories

This mapping will be provided in a future version of this document.

4.2 Mapping Between Reference Design Functions and NIST SP 800-53 Controls

While the Cybersecurity Framework identifies enterprise-level security outcomes, NIST SP 800-53 identifies security controls that apply to systems on which those enterprises are reliant. Which SP 800-53 controls need to be employed depends on system functions and a risk assessment of the perceived impact of loss of system functionality or exposure of information from the system to unauthorized entities. In the case of systems owned by or operated on behalf of federal government enterprises, the risk assessment and applicable SP 800-53 controls are legally mandatory under the Federal Information Security Modernization Act (FISMA) and the Risk Management Framework (RMF). Many other governments and private sector organizations voluntarily employ the RMF and associated SP 800-53 controls.

Table 4-2 provides a mapping between the logical components of the reference design and NIST SP 800-53 security controls. This table indicates how trusted IoT device network layer onboarding and lifecycle management functions help support NIST SP 800-53 controls. Because hundreds of NIST SP 800-53 controls can help support these functions, we have limited use case 2 (see Section 3.1) mappings to those controls on which specified supporting controls directly depend (e.g., dependence of cryptographic protection on key management). Readers needing to determine how their implementations of trusted IoT device network layer onboarding and lifecycle management implementation support RMF processes can refer to the SP 800-53 mappings in Table 4-2.

Table 4-2 Mapping Between Reference Design Logical Components and NIST SP 800-53 Controls

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Creates, signs, and installs the device's unique identity and other birth	Supports (example of) AC-3: Access Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provi-

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	credentials into secure storage. Installs info the device requires for application-layer onboarding (if applicable). Creates a record of devices that it has created.		sioning process. During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. When the device is sold, it will be provided to the device owner. The owner may use this information as the basis of the owner's implementation of connections to the device.
		Supports (example of) AC-4: Information Flow Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, it will be provided to the device owner. The owner may use this information as the basis of the owner's implementation of connections enabling information transmitted by the device.
		Supports (example of) CM-8: System Component Inventory	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, it will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Supports (integral to) IA-3: Device Identification and Authentication	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			the device to have its asserted identity authenticated during onboarding.
		Supports (precedes) IA-9: Service Identification and Authentication	In some application-layer onboarding mechanisms, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service Signed information about the device (e.g., device model, ID, onboarding protocol supported) created and provided by the manufacturer during the factory provisioning process is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices.
		Supports (precedes) PM-5: System Inventory	The owner uses this information in compiling the owner's organization-wide inventories information that includes devices obtained from that manufacturer.
		Supports (precedes) SR-4: Provenance	Creation, signing, and installation of the device's unique identity and other birth credentials into secure storage and creation of records of devices that the manufacturer has created support documentation and maintenance of the valid provenance of system components. During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
		Supports (example of) SR-5: Acquisition Strategies, Tools, and Methods	The signed device identities and records of manufactured devices can be required in acquisition and procurement documents

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			to protect against and mitigate supply chain risks.
		Supports (example of) SR-11: Component Authenticity	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. Signing and installing the device's unique identity and other birth credentials into secure storage supports implementation of anti-counterfeiting policies and procedures by providing means to detect counterfeit components and prevent them from entering the system.
		Is supported by (example of) IA-1: Identification and Authentication Policy and Procedures	Customer policies regarding device access and information flows inform the manufacturer's decisions regarding information to be provided about the device's requirements for application-layer onboarding (e.g., onboarding protocol supported) and recording by the manufacturer during the factory provisioning process. When the device is sold, this information may be provided to the device owner. The owner may use this information as the basis for acquisition, installation, and onboarding decisions.
		Is supported by (precedes) IA-4: Identifier Management	Management of device identifiers communicates to the manufacturer component identification information used to enable a record of devices that it has created to be used to support conformance to acquisition policies and notification agreements.
		Is supported by (precedes) SR-8: Notification Agreements	The role of the manufacturer as established in notification agreements with en-

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			tities involved in the supply chain for systems components must be made clear before it performs factory provisioning so the manufacturer can understand what onboarding-specific hardware, firmware, and software it must integrate into the device
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner, and it may also be the mechanism for providing device ownership information to the device itself. Device bootstrapping information is information (e.g., a public key that pairs with the device's private key) that the device owner requires to perform trusted network-layer onboarding.	Supports (precedes) AC-3: Access Enforcement	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (precedes) AC-4: Information Flow Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. Note that the generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (integral to) CM-8: System Component Inventory	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Supports (example of) IA-1: Identification and	Cryptographically authenticating devices during network-layer onboarding to the

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Authentication Policy and Procedures	device owner's network can facilitate an organization's identification and authentication policies and procedures regarding network connections to IoT devices.
		Supports (integral to) IA-3: Device Identification and Authentication	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (precedes) IA-9: Service Identification and Authentication	Signed device bootstrapping information is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices.
		Supports (precedes) PM-5: System Inventory	The ow uses the bootstrapping information in compiling the owner's organization-wide inventory information that includes devices obtained from that manufacturer.
		Supports (precedes) SR-4: Provenance	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. Creation, signing, and installation of the device's unique identity and other birth credentials into secure storage and creation of records of devices that the manufacturer has created support documentation and maintenance of the valid provenance of system components.
		Supports (example of) SR-5: Acquisition Strategies, Tools, and Methods	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			onboarding to the device owner's network. These signed device identities and records of manufactured devices can be required in acquisition and procurement documents to protect against and mitigate supply chain risks.
		Supports (example of) SR-11: Component Authenticity	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. Signing and installing the device's unique identity and other birth credentials into secure storage may support implementation of anti-counterfeiting policies and procedures by providing means to detect counterfeit components and prevent them from from entering the system.
		Is Supported by (precedes) SR-1: Supply Chain Risk Management Policy and Procedures	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information from the manufacturer to the device owner are informed by supply chain risk management policies and procedures so that the manufacturer can use expected mechanisms to enable policy enforcement (e.g., enrollment of the device's credential into a certificate authority, direct transfer of the bootstrapping information into the device owner's database, or use of a QR code that is imprinted on the device or its packaging).
Network-Layer Onboarding Component	Runs the onboarding protocol to interact with the IoT device to perform one-way	Supports (integral to) AC-1: Access Control Policy and Procedures	The network-layer onboarding service supports implementation of access control policies and procedures by providing authenticated, authorized devices with a network-layer credential.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Supports (integral to) AC-3: Access Enforcement	The network-layer onboarding component supports access enforcement by authenticating a connected IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
		Supports (integral to) AC-17: Remote Access	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The network-layer onboarding component is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Supports (example of) AC-19: Access Control for Mobile Devices	Where the IoT device is a mobile device, remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely.
		Supports (integral to) AC-20: Use of External Systems	Access to the network from external systems is managed by ensuring that only devices that have network-layer credentials are permitted to connect to external systems.
		Supports (integral to) AC-24: Access Control Decisions	Access control decisions are enforced by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely.
		Supports (integral to) IA-1: Identification and Authentication Policy and Procedures	The network-layer onboarding service supports facilitates implementation of identification and authentication policies and procedures by providing a network-layer credential for authentication of authorized devices.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) IA-3: Device Identification and Authentication	The network-layer onboarding service supports device identification and authentication by providing a network-layer credential for authentication of authorized devices.
		Supports (precedes) IA-9: Service Identification and Authentication	Signed information about the device (e.g., device model, ID, onboarding protocol supported) created and provided by the manufacturer during the factory provisioning process is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices. The network-layer onboarding service supports service identification and authentication by providing a network-layer credential for authentication of authorized devices.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The network-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	When a device is onboarded, access control lists (ACLs) and policy for the device are configured on the router or switch to constrain communications to and from the device according to policy.
		Is supported by (precedes) SR-1: Supply Chain Risk Management Policy and Procedures	The network-layer onboarding component of the device owner must be in possession of the device bootstrapping information in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the device owner must be consistent with both manufacturer and customer supply chain risk management policies and procedures.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Is supported by (example of) AT-3: Role-Based Training	In some network-layer onboarding protocols, participation of a trusted onboarder is required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network with the device's bootstrapping information. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
		Is supported by (integral to) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the network-layer onboarding component's establishment of an encrypted channel with the IoT device in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Wireless access point and/or router or switch. The router may get configured with per-device ACLs and role policy when devices are onboarded.	Supports (example of) AC-4: Information Flow Enforcement	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment, thus enforcing approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information flow control policies.
		Supports (example of) AC-5: Separation of Duties	When a device is onboarded, access control lists (ACLs) and policy for the device may be configured on the router or switch to constrain communications to and from the device according to separation of duties policies.
		Supports (example of) AC-6: Least Privilege	When a device is onboarded, access control lists (ACLs) and policy for the device may be configured on the router or switch to constrain communications to and from

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			the device according to least privilege policies.
		Supports (example of) AC-16: Security and Privacy Attributes	When a device is onboarded, access control lists (ACLs) and policy for the device may be configured on the router or switch to constrain communications to and from the device consistent with policies regarding permitted security and privacy attributes.
		Supports (integral to) AC-17: Remote Access	When a device is onboarded, access control lists (ACLs) and policy for the device are configured on the router or switch to constrain communications to and from the device.
		Supports (integral to) AC-24: Access Control Decisions	When a device is onboarded, access control lists (ACLs) and policy for the device are configured on the router or switch to control decisions regarding communications to and from the device.
		Supports (example of) SC-7: Boundary Protection	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	The authorization service provides the network onboarding component and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any special roles or be subject to any specific access controls. The authorization service may	Is supported by (precedes) CM-8: System Component Inventory	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	also help enable the device to determine if the network is authorized to onboard it.		
IoT Device	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the onboarding protocol and interacts with the network onboarding component to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as performing a secure boot process, performing trusted firmware updates, and securely conveying its device intent information.	Supports (integral to) IA-3: Device Identification and Authentication	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of in-formation exchanged (e.g., the device's application-layer credentials).
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Secure Storage	Storage on the IoT device is designed to be protected from unauthorized access and capable of detecting attempts to hack or modify its contents. Used to	Supports (integral to) AC-1: Access Control Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to implementation of the organization's access control policy.
		Supports (integral to) IA-1: Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	store and process private keys, credentials, and other information that must be kept confidential.		to implementation of the organization's identification and authentication policy.
		Supports (integral to) AC-3: Access Enforcement	The secure storage of the device's private key, which serves as its birth credential within the device and binds the device to its credential, is an essential element of the access enforcement mechanism.
		Supports (integral to) IA-1: Policy and Procedures	The secure storage of the device's private key, which serves as its birth credential within the device and binds the device to its credential, is essential to the effective implementation of identification and authentication policies as they relate to IoT.
		Supports (integral to) IA-3: Device Identification and Authentication	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to the effectiveness and security of device identification and authentication processes. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) SC-28: Protection of Information at Rest	Information stored in secure storage is protected from unauthorized access and disclosure.
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (integral to) IA-3: Device Identification and Authentication	The fact that a credential is signed by a trusted CA provides a mechanism for enabling the credential to be verified and revoked that is essential to the integrity of the authentication process.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) IA-3: Device Identification and Authentication	If the device credential is an X.509 certificate (e.g., an IDevID) that is signed by a CA, this certificate binds the device's credential to the device's identity.
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Application-Layer Onboarding Service	After the device connects to the network, this component interacts with the device using an application-layer onboarding protocol to authenticate the device, verify that it is authorized to be application-layer onboarded, establish a secure channel with it, and securely provision application-layer credentials to it. The application-layer credentials will allow the device to authenticate to an application-layer service. The application layer service may be a lifecycle management service that can be used to securely and automatically	Supports (example of) AC-18: Wireless Access	The application-layer onboarding component may establish a wireless encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
		Supports (integral to) IA-3: Device Identification and Authentication	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The application-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
		Is Supported by (precedes) CM-8: System Component Inventory	In some application-layer onboarding mechanisms, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service. The process of application-layer onboarding a device may also serve as an automatic mechanism to inventory and keep

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	update and patch the device on an ongoing basis.		track of which devices have application-related software installed and are therefore capable of interoperating with the application service.
Continuous Authorization Service	Performs a set of ongoing, policy-based assurance and authorization checks on the IoT device to support device lifecycle monitoring and control. For example, it may perform behavioral analysis or device attestation and use the results to determine whether the device should be granted access to certain high-value resources, assign the device to a particular network segment, or take other action.	Supports (example of) RA-2: Security Categorization	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify the impact of system security breaches.
		Supports (example of) RA-3: Risk Assessment	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify potential threats.
		Supports (example of) PM-10: Authorization Process	The ongoing device authorization service may quarantine a device, refuse a device access to the network or to certain high-value resources, or take other pre-defined action based on policy.
		Supports (example of) AC-4: Information Flow Enforcement	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity against a baseline to detect anomalies and events.
		Supports (example of) CM-2: Baseline Configuration	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity against a baseline to detect anomalies and events in order to maintain a baseline configuration.
		Supports (example of) SI-4: System Monitoring	Device lifecycle monitoring may be used to detect attacks and indicators of potential attacks as well as anomalous security configuration changes.
		Supports (example of) CA-7: Continuous Monitoring	The ongoing device authorization service may collect and correlate data from device attestation services, behavioral analytics tools, authentication services, and other sources as input to its policy-based assessment of device authorization.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) IR-4: Incident Handling	If the policy-based assessment of the device does not meet a given threshold, the device may not be authorized to access specific resources or the network itself. If the assessment of the device's trustworthiness does not meet a given threshold and, as a result, the device is denied access to the network or other resources, such restriction may help contain incidents that involve the device.

4.2.1 Mapping between Build 1 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

4.2.2 Mapping between Build 2 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

Appendix A References

[1] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,* National Institute of Standards and Technology, Gaithersburg, MD, April 2018, 48 pp. Available: https://doi.org/10.6028/NIST.CSWP.04162018

[2] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Gaithersburg, MD, September 2020, 465 pp. Available: https://doi.org/10.6028/NIST.SP.800-53r5