ETSI TR 103 305-3 V3.1.1 (2023-07)

TECHNICAL REPORT

Cyber Security (CYBER);
Critical Security Controls for Effective Cyber Defence;
Part 3: Internet of Things Sector

Reference

RTR/CYBER-00107

Keywords

cyber security, cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 3 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.9].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Internet of Things (IoT) networks, devices and applications have become pervasive worldwide as a critical infrastructure sector. The protection of this infrastructure from cyber security threats by instituting effective risk control and enhanced resilience has received the global attention of governmental authorities and industry organizations [i.1] thru [i.16]. The present document addresses this protection challenge by providing guidance on individually applying the most current version of the Critical Security Controls for effective cyber defence to IoT by enterprises. For compliance purposes, the Critical Security Controls have mappings to almost every known government and industry cyber security framework with extensive implementations for diverse operating systems and applications. The present document is directed at enterprise IoT and not intended as an alternative to ETSI normative consumer IoT specifications, but may supplement their use, ETSI EN 303 645 [i.13] and ETSI TS 103 701 [i.14].

Introduction

The Critical Security Controls are a prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. Under the auspices of the Center for Internet Security (CIS), the Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the Controls come from a wide range of sectors including, retail, manufacturing, healthcare, education, government, defence, and others. While the Controls address the general practices that most enterprises should take to secure their systems, some operational environments may present unique requirements not addressed by the Controls.

A significant evolution of cyber defence is now underway. To help better understand cyber threats, an array of threat information feeds, reports, tools, alert services, standards, and threat-sharing frameworks have emerged. This information is immersed in an ecosystem of security requirements, risk management frameworks, compliance regimes, and regulatory mandates. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure. However, all of this technology, information, and oversight has become a veritable "Fog of More" - competing options, priorities, opinions, and claims that can paralyse or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings great benefits, but it also means that the data and applications are distributed across multiple locations, many of which are not within the enterprise infrastructure.

The Controls started as a grassroots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. This clause breaks down and map the applicable Controls and their implementation for the cloud environment. As the Controls continue to be refined and re-worked through the expert community, the call for Controls guidance for the IoT sector became a high priority.

1 Scope

The present document is an evolving repository for guidelines on service sector Critical Security Control implementations. Because of its rapidly scaling importance and need for defensive measures, the enterprise Internet of Things (IoT) sector are treated here. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks.

The present document is technically equivalent and compatible with the "CIS Controls v8 IoT Companion Guide" [i.16].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[i.2] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

[i.3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[i.4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).

[i.5] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[i.6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[i.7] 2022/0272 (COD): Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[i.8] Commission Staff Working Document Advancing the Internet of Things in Europe Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market.

[i.9] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.10] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.11] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.12] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.13] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.14] ETSI TS 103 701: "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.15] ETSI TR 103 621: "Guide to Cyber Security for Consumer Internet of Things".

[i.16] Center for Internet Security (CIS): "CIS Controls v8 Internet of Things Companion Guide".

[i.17] The Internet of Things: An Overview: "Understanding the Issues and Challenges of a More Connected World".

[i.18] IEEE®: "Towards a Definition of the Internet of Things (IoT)".

[i.19] Gartner®'s IT Glossary: Internet of Things (IoT).

[i.20] NIST® SP 800-160 Vol. 1 Rev. 1: "Engineering Trustworthy Secure Systems".

[i.21] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[i.22] NIST® SP 800-63-3: "Digital Identity Guidelines".

[i.23] IETF RFC 8520: "Manufacturer Usage Description Specification".

[i.24] NIST® SP 1800-15: "Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)".

[i.25] W3C® Recommendation 8 April 2021: "Web Authentication: An API for accessing Public Key Credentials Level 2".

[i.26] IETF RFC 7744: " Use Cases for Authentication and Authorization in Constrained Environments".

[i.27] IEEE®: "DDoS in the IoT: Mirai and Other Botnets".

[i.28] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector".

[i.29] IEEE 802.1x™: "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control".

[i.30] OWASP® IoT Project: Guidance for assessing and developing IoT devices.

[i.31] FIRST: "Common Vulnerability Scoring System (CVSS) SIG".

[i.32] IoT Penetration Testing Guide, Aditya Gupta.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 303 645 [i.13], ETSI TS 103 701 [i.14] and ETSI TR 103 621 [i.15] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Network
AAA	Authentication, Authorization, and Auditing
ACK	Acknowledge
AD	Active Directory
API	Application Programming Interface
ARP	Address Resolution Protocol
CBOR	Concise Binary Object Representation
CIS	Center for Internet Security
COOP	Continuity Of Operations Planning
COSE	CBOR Object Signing and Encryption
CSC	Critical Security Control
cTLS	compact Transport Layer Security
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DSS	Data Security Standard
dTLS	datagram Transport Layer Security
EDHOC	Ephemeral Diffie-Hellman Over COSE
EMM	Enterprise Mobility Management
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IG	Implementation Groups
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
ISAC	Information Sharing & Analysis Center
IT	Information Technology
JTAG	Joint Test Action Group
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control (address)
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MUD	Manufacturer Usage Description
N/A	Not Applicable

NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operating System
OSCORE	Object Security for Constrained RESTful Environments
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
pen	penetration
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RESTful	Representational State Transfer
RF	Radio Frequency
RFID	Radio Frequency Identifier
RSU	Roadside Unit
RTOS	Real-Time Operating System
SD	Secure Digital
SIEM	Security Information and Event Management
SoHo	Small office Home office
SSID	Service Set Identifier
SYN	Synchronization
TCP	Transmission Control Protocol
TTPs	Tactics, Techniques, and Procedures
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi®	Wireless Fidelity

4 Applying the Critical Security Controls for effective risk control and enhanced resilience of the Internet of Things sector

4.1 Introduction, Methodology and Use

The purpose of the Controls Internet of Things Community is to develop best practices and guidance for implementing the Controls in association with a variety of devices within the Internet of Things (IoT). Enterprise use of IoT presents unique and complex challenges for security professionals. IoT devices are being embedded into the enterprise across the globe and often cannot be secured via standard enterprise security methods, such as running a monitoring application on the device, as the devices cannot support these types of applications. Yet for ease of use, enterprise IoT devices are often connected to the same networks that employees use day in and day out and are often directly connected to the internet via a variety of network protocols (e.g. Ethernet, Bluetooth®, Wireless Fidelity (Wi-Fi®), cellular).

Definition of Internet of Things

There is no universally agreeable definition for IoT. The variety of perspectives from industry, academia, governments, and others across the world have led to different definitions, each focused on the needs of their sector, business, or area of interest. Each definition has relevant strengths and weaknesses, and they do not act to invalidate each other. Instead, these definitions work within their desired context, and others may choose to use and apply them as they see fit for the systems that will be procured and implemented.

- In The Internet of Things: An Overview [i.17], a 2015 report from The Internet Society, IoT is defined as: "*…scenarios where network connectivity and computing capability extends to objects, sensors, and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human intervention*".

- A 2015 report from the Institute of Electrical and Electronics Engineers Incorporated (IEEE), titled *Towards a Definition of the Internet of Things* [i.18], defines IoT as "*A network of items - each embedded with sensors - which are connected to the Internet*".

- IoT has been defined within a recommendation from the International Telecommunication Union as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*".

- Gartner's IT Glossary [i.19] defines IoT as "*the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment*".

Regardless of which definition an enterprise chooses to use, there are certain common features:

- Communications - Whether this is via a local medium, such as Radio Frequency Identification (RFID), Bluetooth, Wi-Fi, or via a Wide Area Network (WAN) protocol, such as cellular, IoT devices can communicate with other devices.

- Functionality - IoT devices have a core function as well as some additional functionality but they do not do everything. Most IoT devices do one thing and do it well.

- Processing capability - IoT devices have sufficient processing capability to make their own decisions and act on inputs received from outside sources, but not enough intelligence to do complex tasks. For instance, they generally cannot run a rich operating system designed for a traditional desktop or mobile device.

The lack of a consistent, agreed-upon definition is actually part of the challenge within the IoT arena. IoT is a large, complex space and common issues include:

- Ubiquity - There are a large number of overall devices.

- Diversity - Devices are developed by different manufacturers with varying version numbers of hardware, firmware, and software.

- Ecosystem - Multiple vendors are involved in creating each device, including hardware, firmware, and software.

- Standardization - There are minimal agreed standards for securing access and communications for these devices.

Examples of IoT devices that might be included within an enterprise include speakers, security cameras, door locks, window sensors, thermostats, headsets, watches, power strips, and more basically any device that may be integrated into a typical business IT environment.

Methodology

A consistent approach is needed for analysing the Controls in the context of IoT. For each of the 18 Controls, the following information is provided in the present document:

- Applicability - This assesses the degree to which a Control functions or pertains to IoT.

- Challenges - These are unique issues that make implementing any of the relevant Controls, or associated Safeguards, for IoT devices difficult.

- Additional Discussion- A general guidance area to include relevant tools, products, or threat information that could be of use can be found here.

Scope

The objective of this guide is to have broad applicability across sectors. IoT affects all areas of computing across multiple sectors, such as healthcare, aviation, public safety, and energy. This has led to sector-specific IoT security guidance, but the present document is purposefully sector-agnostic. As such, this guide focuses on purchasing, deploying, and monitoring commercially available IoT devices. It does not provide guidance on how to design, develop, and manufacture secure IoT devices, such as the secure system development process noted within National Institute of Standards and Technology (NIST®) Special Publication SP 800-160 Vol.1 Rev. 1 [i.20].

The Implementation Groups (IG) are a guideline to help enterprises determine a starting point for implementation of the Controls. This guide does not re-group the Safeguards for IoT, and instead maintains the same prioritization used in the Controls. Enterprises will, at times, find the need to implement Safeguards in a higher IG. When integrating new technology into an environment, such as IoT, an enterprise should fully consider, and assess the security risks and impacts to assets and data; that understanding should drive the selection and implementation of appropriate Safeguards regardless of IG.

Terminology

As noted earlier, there are many definitions of IoT. Below are basic descriptions of IoT components and terminology are used throughout this guide. Devices are the *things* within *IoT* and are the primary focus of this guide. Gateways are devices that multiple things connect to in order to receive instructions, transfer data, etc. Multiple devices are often connected to a single gateway, or a gateway may passively monitor IoT devices. A gateway has an internet connection, whereas not all IoT devices will, and may only support local wireless protocols such as RFID, Wi-Fi, Bluetooth, and Zigbee; or may be used over wide area networks such as LoraWAN.

Gateways, and other types of edge IoT devices often transition from a constrained set of devices and protocols to a less constrained environment. Gateways are one way to help reduce the attack surface of legacy IoT devices that cannot be properly secured. Many consumer IoT devices are associated with complex cloud platforms that can control the behavior of IoT devices and access and store data.

4.2 Applicability Overview

■ More than 60 % of Safeguards apply

▨ Between 60 % and 0 % of Safeguards apply

□ 0 % of Safeguards apply

Control	Framework Title	Applicability
1	Inventory and Control of Enterprise Assets	■
2	Inventory and Control of Software Assets	▨
3	Data Protection	■
4	Secure Configuration of Enterprise Assets and Software	▨
5	Account Management	■
6	Access Control Management	▨
7	Continuous Vulnerability Management	■
8	Audit Log Management	■
9	Email and Web Browser Protections	▨
10	Malware Defences	■
11	Data Recovery	■
12	Network Infrastructure Management	■
13	Network Monitoring and Defence	■
14	Security Awareness and Skills Training	■
15	Service Provider Management	■
16	Application Software Security	■
17	Incident Response Management	■
18	Penetration Testing	■

4.3 Applying the Critical Security Controls and Safeguards

4.3.1 CONTROL 01 Inventory and Control of Enterprise Assets

IoT Applicability

It is important to track which devices have access to the network and are accessing data and enterprise resources. IoT devices are no different and this Control is considered extremely important. Traditional Media Access Control (MAC) and Internet Protocol (IP) addresses can be used for device identifiers. Unfortunately, not all IoT devices will have these identifiers present (e.g. MAC address, IP address). For instance, while Zigbee devices support a physical layer MAC address, they use a Zigbee network address in lieu of an IP address. Very simple sensors and devices used for location tracking may only beacon identifiers for RFID. When using devices that do not support network-based authentication, network segmentation can be considered as a possible way to mitigate risk.

IoT Challenges

Enterprises should deploy technology that tracks the myriad of IoT devices which can be deployed across their enterprise. Understanding the device types and, in some cases, which specific devices are authorized to connect to the network is the starting point to adapting this Control for IoT. To the extent practical, this Control should be limited to enterprise assets and assets that connect to the enterprise network. For devices without traditional identifiers, physical tags can be placed onto the devices themselves that integrate with asset management systems. In order to preserve privacy, these tags should not identify the organization. For some IoT devices with an externally accessible physical interface, cellular devices may be inserted into the device to allow ~~it~~ to be included in a cloud-based asset management system.

Some IoT devices are designed to work in relative isolation and never connect to an enterprise network. These devices still may be network-connected though, as they can communicate with a back-end cloud platform that the enterprise neither controls nor manages. Wireless IoT gateways can also be used to monitor wireless traffic from IoT devices. This information can then be relayed to an asset management system, either in the cloud or physically hosted at the enterprise. Another challenge ~~is~~ using digital certificates in IoT devices. Finally, Global Positioning System (GPS) can also be an effective way to monitor the location of IoT devices distributed outside the enterprise.

IoT Additional Discussion

Typical asset tracking tools may not work out of the box with IoT devices. Network scans for legacy and non-traditional devices may be dangerous to device, network, and system stability, potentially leaving IoT endpoints in an error state. Before purchasing devices and using them within an enterprise, it is worthwhile to understand how a device will respond to an asset discovery tool, and how well it will integrate with any asset management tools being utilized by an enterprise. The conventional approach of using ping responses, Transmission Control Protocol Synchronization (TCP SYN) or Acknowledge (ACK) scans can disrupt communications or, in some cases, even impact device operations. Passive methods are preferred and are less likely to impact system availability or interact with vendor systems in a manner that could cause warranty issues. Where practical, non-intrusive methods should be leveraged, including Media Access Control-Address Resolution Protocol (MAC-ARP) tables, Domain Name System (DNS), Active Directory (AD), or a variety of IoT-specific tools employed to control and collect data in these systems for the express purpose of locating the variety of connected assets.

Wireless monitoring may be necessary to identify devices, as many IoT devices lack wired physical connections. Many newer IoT devices support integration into IoT management systems via Application Programming Interfaces (APIs). At the very least, enterprises can create a listing of device MAC address, device type, serial number, and other relevant information. "Smarter" IoT devices can utilize digital certificates to enhance identity and access management.

Control 1: Inventory and Control of Enterprise Assets					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	See [i.10]	●	●	●	Y	Hardware inventories are important for any device accessing the enterprise network, and IoT devices should be included in this inventory. Alongside the information listed in the text of the Safeguard, any other information physically attached to the hardware may need to be tracked, such as HomeKit information, connection methodology, and gateway type.
1.2	Devices	Respond	Address Unauthorized Assets	See [i.10]	●	●	●	Y	Unknown IoT devices and gateways connected to enterprise networks and systems should be quickly investigated and removed.
1.3	Devices	Detect	Utilize an Active Discovery Tool	See [i.10]		●	●	Y	Active discovery tools should be implemented to identify IoT devices, although some types of scans could leave devices in a non-functional state or affect essential IoT device communications. The types of scans run against high-value or critical IoT assets should be contemplated before they are run, with the expected outcomes identified beforehand. Testing can occur before putting the device into the network.
1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	See [i.10]		●	●	Y	This Safeguard should be applicable to IoT devices using Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). Although possible, it is not considered an industry-accepted method of tracking IoT device inventory and should not be the primary method in which IoT devices are tracked.
1.5	Devices	Detect	Use a Passive Asset Discovery Tool	See [i.10]			●	N	A passive asset discovery tool may not identify all IoT devices, yet can be a solid step forward to understanding the devices on the network.

4.3.2 CONTROL 02 Inventory and Control of Software Assets

IoT Applicability

Network scanning and agent-based approaches are typical methods for software asset management. As mentioned in Control 1, network scanning can leave many IoT devices in an unsafe or unusable state. Agent-based approaches will be ineffectual for IoT devices as there is not a common platform for the agent to be installed on the device. Manual and procedural methods can be used for asset tracking, for example a spreadsheet.

IoT Challenges

Identifying the versions of firmware of IoT devices within the enterprise is a challenge. It may be possible to leverage central command and control systems, which are aware of device firmware versions. However, custom and restricted operating systems may limit remote query capability. In general, IoT device firmware is not patchable, but it is loaded onto the device as a new complete image. To obtain the listing of firmware applications on an embedded device, it may be necessary to work with the device developer/manufacturer. Manual sampling or firmware extraction via on-board direct maintenance ports (e.g. Joint Test Action Group (JTAG)) using proprietary software and hardware tools may be required.

IoT Additional Discussion

In many cases, firmware should be delivered over the network to IoT devices. This often includes verifying digital signatures as part of the installation of firmware. To the extent practical, utilize best practices for securing firmware images, which often includes applying digital signatures that are evaluated by the device before loading. The user or the device may check the firmware signature. This may require a secured space within the device to store credentials used for signature validation. Understanding the firmware update procedure before purchasing the device is best practice in these situations, since firmware cannot be changed after the fact.

Tracking versions of Bluetooth and Wi-Fi in devices can be quite difficult and may not be possible using traditional scanning methods. Applications like Airodump-ng for Wi-Fi devices and hcitool or ubertooth-scan for Bluetooth devices will provide broadcast advertisements and MAC addresses. Note that for Bluetooth devices, MAC addresses do not conform to typical conventions and are oftentimes represented as the device Wi-Fi MAC address incremented by 1 bit. The information available from Wi-Fi and Bluetooth advertisements will allow enterprises to identify which versions of wireless protocols are supported. Allowlisting is generally not available on IoT devices. Allowlisting can occur at the application layer, or specific libraries or scripts can be allowlisted. A more common capability is for devices to perform *command allowlisting*, which only specifies a subset of commands that a device would accept. This will more likely be available with IoT vendors that engage within a security engineering process over the life cycle of the product.

Control 2: Inventory and Control of Software Assets					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
2.1	Applications	Identify	Establish and Maintain a Software Inventory	See [i.10]	●	●	●	Y	At minimum, a listing of the firmware versions associated with the IoT device can be noted. This should include firmware and platform versions.
2.2	Applications	Identify	Ensure Authorized Software Is currently supported	See [i.10]	●	●	●	Y	Enterprises should check the period of time for which a device will be supported before purchase. Additional support may be available for purchase, but this is uncommon.
2.3	Applications	Respond	Address Unauthorized Software	See [i.10]	●	●	●	N	Firmware that is not approved by the enterprise should be removed. Unfortunately, enterprises are often unable to control the software that is running on an IoT device.
2.4	Applications	Detect	Utilize Automated Software Inventory Tools	See [i.10]		●	●	N	Not all IoT devices will be able to integrate or be inventoried by an automated tool, but those that have this capability should use it.
2.5	Applications	Protect	Allowlist Authorized Software	See [i.10]		●	●	N	This capability is unavailable on most IoT devices, many of which will lack the processing power or security architecture to perform allowlisting.
2.6	Applications	Protect	Allowlist Authorized Libraries	See [i.10]		●	●	N	Allowlisting individual libraries is typically not available on IoT devices.
2.7	Applications	Protect	Allowlist Authorized Scripts	See [i.10]			●	N	Allowlisting individual scripts is typically not available on IoT devices.