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.

4.3.3 CONTROL 03 Data Protection

IoT Applicability

Protecting the security of data being stored, transmitted, and manipulated on IoT devices can be critical depending on use case or sector. Certain industries may not contain any sensitive data in the traditional sense. In other instances, certain IoT devices will be dedicated to environments that have an informal set of standards and norms, or their usage may be directly regulated (e.g. Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR)). The level of data protection needed is often specific to the use case at hand, depending on factors such as data sensitivity and likelihood of exposure.

Some IoT devices will process and transmit complex enterprise or customer information in modern formats, whereas other devices will read and transmit physical attributes such as temperature or pressure. This latter information is sometimes not deemed to be especially sensitive or proprietary on its own, though it may become more sensitive when coupled with other data points, such as location or identifiers used for people. In some cases, these "simple" IoT use cases can be absent of any particular protections in the way it is collected, transferred, stored, and analysed.

IoT Challenges

Detecting and preventing the flow of data out of IoT devices is a difficult task, as is preventing Unauthorized disclosure. IoT devices will often have a diverse supply chain, utilizing numerous hardware manufacturers, all of which will leverage cloud platforms. This makes data protection quite difficult for the menagerie of IoT devices in use. If possible, data-in-transit security, through protocols such as compact Transport Layer Security (cTLS), should be implemented to guard against eavesdropping on data flowing between IoT and other enterprise components. Although IPSec would be an excellent alternative, it is unlikely to be supported on an IoT device. This is difficult as most IoT devices will ship with a set of security protocols that are supported which may never change over the lifetime of the device.

Protections should also be implemented for the data stored on any cloud platform or the device itself, including integrated memory or removable storage media. This is another area typically outside of enterprise control and may need to be screened for pre-purchase. The same can be said for any IoT device's ability to manage cryptographic keys. This is further addressed in Control 15: Service Provider Management.

IoT Additional Discussion

Legacy or low-end IoT devices often do not encrypt data in transit or in storage. Typically, IoT traffic is perishable, near real-time, of limited historical value, and tolerant of loss. Sophisticated attacks looking to manipulate data often require deep system knowledge and serious mission benefit to justify the cost of technique and exploit development. In cases where actual threats or observed threat intelligence indicates the need, methods such as multi-path redundancy, cross-sensor correlation, or a custom in-line device may be put into place. Many IoT devices will attempt to store data in the cloud by default without enterprise approval. This may also include storing data on any mobile devices used to control a device. This makes data protection hard, as enterprises may not have visibility into what information is being transmitted.

Traditional enterprise Data Loss Prevention (DLP) systems can be helpful for email and network stored data. It is important to perform methodical threat modeling for every new IoT system being implemented. Consider the value of data when determining whether encryption should be applied to protect that data. In some instances, the need to support near real-time communications outweighs the need to apply an encryption layer to the data. The output of a threat analysis will provide the foundation for an effective data protection strategy.

Control 3: Data Protection					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
3.1	Data	Identify	Establish and Maintain a Data Management Process	See [i.10]	●	●	●	Y	The elements of the data management process mentioned in this Safeguard description can all apply to IoT. It is possible that these can be addressed as a subcomponent of an IoT Security Policy, or possibly addressed as part of Data Management.
3.2	Data	Identify	Establish and Maintain a Data Inventory	See [i.10]	●	●	●	Y	Sensitive information on IoT and associated management platforms should be understood and inventoried. This Includes data passing through the system and data recorded by various onboard sensors.
3.3	Data	Protect	Configure Data Access Control Lists	See [i.10]	●	●	●	Y	IT administrators may be able to control access and lifetime of accounts via administrative consoles if an IoT device's manufacturer provides an app or other management interface. If this is supported, access should be controlled.
3.4	Data	Protect	Enforce Data Retention	See [i.10]	●	●	●	Y	IT administrators may be able to control access and lifetime of accounts via administrative consoles. This will depend on the device and platform.
3.5	Data	Protect	Securely Dispose of Data	See [i.10]	●	●	●	Y	This can be difficult for IoT devices that require access to specific cloud platforms. Not all devices will provide the ability to delete the data stored on the device. Device destruction may be necessary.
3.6	Devices	Protect	Encrypt Data on End-User Devices	See [i.10]	●	●	●	N	IoT devices are typically not considered end-user devices. With that said, corporate sensitive data including hours of operation or access, information collected via sensors or cameras may be stored and are likely worth protecting. Object Security for Constrained RESTful Environments (OSCORE) may be a useful solution. See [i.21].
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	See [i.10]		●	●	Y	Data classification decisions should be explicitly made for IoT data, to include data stored on, or downloaded from, their management platforms.
3.8	Data	Identify	Document Data Flows	See [i.10]		●	●	Y	The enterprise should understand how sensitive data is transferred to and from IoT devices, apps, and cloud-based platforms.

Control 3: Data Protection					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
3.9	Data	Protect	Encrypt Data on Removable Media	See [i.10]		●	●	Y	IoT devices do not commonly utilize USB storage; however, other removable storage media (such as SD cards) might be used to store video files, telemetry, or even the operating system of the IoT device. Based on the sensitivity of stored data, encryption should be used to mitigate risks related to data theft and disclosure.
3.10	Data	Protect	Encrypt Sensitive Data in Transit	See [i.10]		●	●	Y	This is an important Safeguard for IoT devices, but enterprises will need to verify if this capability is available for the specific device before device purchase.
3.11	Data	Protect	Encrypt Sensitive Data at Rest	See [i.10]		●	●	Y	This is an important Safeguard for IoT devices, but enterprises will need to verify if this capability is available for the specific device, and within the device management platform, before device purchase.
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity	See [i.10]		●	●	Y	The use of network segmentation strategies is strongly recommended to keep IoT components operating in their own zones or on their own separate networks. This concept applies to this Safeguard as well. IoT data processing and storage will typically not be a highly sensitive computing activity and should be kept separate. Deliberate decisions should be made as to where and how IoT gateways should be segmented.
3.13	Data	Protect	Deploy a Data Loss Prevention Solution	See [i.10]			●	N	Traditional enterprise Data Loss Prevention (DLP) can be helpful for email and network stored data, but cloud applications and data may be more difficult to get visibility from IoT devices. There are tools that leverage cloud service APIs to gain this visibility, or filtering clouds that proxy IoT services.
3.14	Data	Detect	Log Sensitive Data Access	See [i.10]			●	Y	IoT devices themselves are likely going to be unable to log sensitive data access within their own system, but enterprises can log which systems and datastores an IoT device accesses.

4.3.4 CONTROL 04 Secure Configuration of Enterprise Assets and Software

IoT Applicability

A majority of the time, resource constrained IoT devices lack the configuration and customization options provided by laptops or even mobile devices. These configuration and customization options are essential to device hardening and secure configuration. Yet some IoT devices can still be hardened in a limited fashion. This is true even of embedded IoT devices. A common example is changing default passwords. End users should familiarize themselves with the developers' or manufacturers' documentation in order to take advantage of other available resources (e.g. academic papers, conference proceedings) to understand what configuration options are available and whether a device can be sufficiently configured to meet the needs.

IoT Challenges

A device or application's configuration may drift over time, even if efforts are made to properly configure the device before or during deployment. This could be due to firmware updates, factory resets, or potentially even software errors. Some IoT device configurations, especially for consumer or typical enterprise use, are *solely* available within a corresponding mobile application. Users will need to first connect the device to the application before configuration is an option. Although this can make device configuration, monitoring, and maintenance easier, it also expands the overall attack surface of the device as now the mobile device (and mobile application) should also be secured.

Undocumented APIs, service provider, and developer backdoors may offer Original Equipment Manufacturers (OEMs) and potentially malicious parties' access to the device, and subsequently consumer or enterprise information. For instance, many IoT devices run a web server with network troubleshooting tools installed (e.g. *ping*, *nslookup*) that can be used to profile any internal or external network to which the IoT device is connected. Monitoring what network services an IoT device responds to is necessary as these devices should not be considered trusted until after extensive vetting has occurred.

IoT Additional Discussion

IoT devices sold and marketed as "appliances" with integrated software generally contain proprietary firmware components, limiting applicability of post-development hardening. When configuration options are available, cybersecurity professionals should review and decide if any particular configurations are untenable for the organization. Additionally, if a certain configuration setting is required to assure the security of the component on the network, then that should also be documented. Cybersecurity professionals should baseline these configurations and keep them documented as best practices. This information can be helpful as requirements when selecting future devices.

A subset of IoT devices support Real-Time Operating Systems (RTOSs) that allow for some amount of persistent storage. Oftentimes, this persistence comes in the form of startup scripts that can be modified to affect the configuration of the device at boot time. It is worthwhile to take the time to research if these configurations are written in a secure manner. When IoT devices support access control via user or administrator accounts and passwords, default accounts and passwords should be changed in accordance with modern guidelines. If available, Multi-Factor Authentication (MFA) should be used to protect administrator accounts.

Control 4: Secure Configuration of Enterprise Assets and Software					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	See [i.10]	●	●	●	Y	Secure configurations generally cannot be established in the same manner as traditional operating systems or applications. With that said, there may be certain configuration options available such as changing a default password or ensuring MFA is used to access any management functions.
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	See [i.10]	●	●	●	N	IoT devices may need hubs or gateways to function. These devices are often treated like IoT devices themselves. Managing network infrastructure is out of scope for this IoT-based guide.
4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	See [i.10]	●	●	●	N	This is not applicable to IoT devices as they are often headless.
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	See [i.10]	●	●	●	N	There are no IoT considerations for this Safeguard if MUD is not in use. Enterprises leveraging MUD will need to ensure MUD logic is properly set up and configured within network devices.
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	See [i.10]	●	●	●	N	IoT devices do not typically contain an on-device firewall. Devices leveraging MUD will need to ensure MUD logic is properly set up and configured on each IoT device in question.
4.6	Network	Protect	Securely Manage Enterprise Assets and Software	See [i.10]	●	●	●	Y	Software development teams designing IoT devices and infrastructure should use modern, secure management protocols. Research should be done beforehand to make sure IoT devices use secure communication protocols before purchase, such as dTLS, cTLS, EDHOC, and OSCORE.
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	See [i.10]	●	●	●	N	This level of interaction is often not exposed on an IoT device. However, this should be established and appropriate management processes implemented where this level of access is available.

Control 4: Secure Configuration of Enterprise Assets and Software					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications	See [i.10]		●	●	N	IoT devices typically do not offer this level of feature granularity to IT administrators.
4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	See [i.10]		●	●	N	This is a network-level mitigation, out of scope for IoT.
4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	See [i.10]		●	●	N	IoT devices often will not have this feature available as they are often headless.
4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	See [i.10]		●	●	N	If remote wipe is a necessary capability needed for the enterprise, this feature needs to be verified before purchasing. Some IoT devices that support EMM/MDM allow for remote wipe. It is not a common feature.
4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	See [i.10]			●	N	This is not applicable to IoT devices.

4.3.5 CONTROL 05 Account Management

IoT Applicability

IoT devices will have a series of accounts already created and in use when the device is purchased and shipped. Account management is applicable to the mobile applications, devices, and cloud platforms all used for IoT. Additionally, enterprises and potentially individual users may also create new accounts. All of these accounts need to be actively managed. It is uncommon for IoT devices to feature dedicated administrative accounts that are separate from user accounts, for managing IoT devices. In some situations, especially with enterprise or consumer-grade IoT devices, control or pseudo-administrative access can be obtained through management applications on mobile devices.

IoT Challenges

When evaluating IoT components for use in the enterprise, investigate the supported features associated with administrative accounts. This should include the type of authentication credentials and protocols supported by the device and its associated ecosystem. This will most likely include passwords and the strength of the authentication implementation. For administrator accounts, attempt to ensure that at a minimum, strong password requirements are used, and account access is audited. In addition, when feasible, attach the IoT component to a directory, allowing for the use of domain administrator accounts when needed. This will allow for the ability to more easily restrict the use of administrative privileges.

Administrators should be extremely careful when first working with a completely unmanaged device. Some IoT devices are beginning to support some form of Enterprise Mobility Management (EMM) or Unified Endpoint Management (UEM). These technologies allow specific policies and configurations to be sent to an IoT device. General administrative activities can also be performed, such as restarts and diagnosing problems. Administrative accounts can be set up for each device, with credentials managed through that technology portal.

IoT Additional Discussion

Many IoT devices are deployed in insecure areas (e.g. roadside units, or RSUs, in the transportation sector). These devices are sometimes deployed with shared accounts that are used by technicians to manage the devices. Consider alternative methods for restricting administrative access to these types of devices. For legacy devices without privileged access capability, a compensating control may need be applied, such as additional physical security. Newly designed IoT devices and subsystems should integrate use of this Control.

Attackers may attempt to obtain administrator rights to IoT devices via Operating System (OS) or firmware level vulnerabilities so they can hide themselves from the user. This entire Control is difficult to enforce on a rooted device that has its security architecture broken. Although this security architecture bypass may provide a user with root access, they often have default administrator credentials that do not frequently change. Furthermore, if an administrator is able to change their password, it is recommended they comply with the password recommendations set forth by National Institute of Standards and Technology (NIST®) SP 800-63-3 [i.22]. This means that in most situations, memorized secrets (i.e. passwords) chosen by a subscriber (i.e. human) should be at least eight characters long. To the extent practical in IoT, multi-factor authentication (MFA) should always be used. With that said, the overall goal would be to implement authentication solutions that prevent credential theft. This more abstract goal supports PKI, WebAuthn [i.25], and MFA solutions that might only be a password and PIN, which is not preferable to the first two options.

Control 5: Account Management					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	See [i.10]	●	●	●	Y	If an IoT management system or UEM integration is available, which is rare, an inventory of the account accessing that system should be maintained. Local administrative accounts are often not available to be easily inventoried within IoT.
5.2	Users	Protect	Use Unique Passwords	See [i.10]	●	●	●	Y	Administrative accounts for management, and any account used on the device, should use unique passwords.
5.3	Users	Respond	Disable Dormant Accounts	See [i.10]	●	●	●	Y	In a manner similar to traditional systems, dormant accounts should be disabled after a pre-defined time of inactivity wherever this is practical.
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	See [i.10]	●	●	●	Y	Administrative accounts for management should have dedicated passwords. Scheduled auditing of administrative accounts should be regularly performed to assess if admin accounts/privileges are still required. Unfortunately, this is not supported on all IoT devices.
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts	See [i.10]		●	●	Y	If a management technology such as UEM is used, this could obviate the need for local administrative accounts. All management accounts should be inventoried alongside any necessary mobile/cloud applications needed to make the device function.
5.6	Users	Protect	Centralize Account Management	See [i.10]		●	●	Y	Some IoT management technology can integrate with identity service providers, or may provide their own identity service. This is difficult to accomplish on IoT.

4.3.6 CONTROL 06 Access Management Control

IoT Applicability

IoT devices require access management, but often in a different manner than traditional user account management. This is due to the fact that users do not often access an interface, or there is no user account needed to interact with the device (e.g. "Turn on the lights"). The Access Control Management is meant to manage how a user accesses a device all the way through revoking access credentials and privileges. Thorough implementations of Control 5 and Control 6 involve written policies addressing these areas before devices are provided to users. Although that is not always practical for IoT when devices have already been purchased, set up, and are running on an enterprise network.

IoT Challenges

It can be challenging to manage accounts on a device with preset user accounts developed by different vendors. Realistically, it may not be possible to manage all accounts on a device from all of the independent companies involved in development. The accounts may not be properly documented upon receipt of a device, although obtaining a thorough inventory of identifiable accounts is important. It is difficult to identify all root accounts that a developer may use, and it may be preferable to use devices that can disable all accounts that the organization has not explicitly approved. Realistically, it will not be possible to manage all accounts and credentials on an IoT device, yet best efforts are worth the effort.

IoT Additional Discussion

Registering devices within an enterprise directory system such as Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) may be a valid method for restricting access and for effectively monitoring who has authenticated to the devices. However, this is only applicable for those devices that can be configured for AD. Enterprises should ensure that IoT implementation plans include strategies for authentication and monitoring the accounts used to access devices. This data should then be fed back to the SIEM for monitoring and control when IoT devices are incorporated into the enterprise network. Administrators should regularly review user accounts on all systems utilized by the enterprise. Privileges should be adjusted accordingly on a regular basis with over-privileged users addressed and accounts deactivated when necessary.

Legacy IoT systems with stand-alone consolidating or command and control hosts should leverage system tools, augmenting them with manual recording and audit processes as required, to enable this Control. Cloud-based applications supported by the enterprise should be monitored and have their credentials disabled during employee separation. Enterprise applications should be analyzed and reviewed for proper authentication techniques. Special attention should be paid to areas where integration occurs between third-party services and when identities are federated. Logging should be enabled within back-end management services to monitor activity, with the logs regularly reviewed.

Control 6: Access Management Control					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
6.1	Users	Protect	Establish an Access Granting Process	See [i.10]	●	●	●	Y	Written policies should exist for onboarding a new IoT. This should include security requirements reviewed before purchase and rules for who can manage IoT devices.
6.2	Users	Protect	Establish an Access Revoking Process	See [i.10]	●	●	●	Y	In addition to typical workstations and servers, administrators should define this process specifically for IoT devices, apps, gateways, and their management platforms.
6.3	Users	Protect	Require MFA for Externally Exposed Applications	See [i.10]	●	●	●	N	Where possible, MFA should be performed for IoT cloud-based applications. Generally, IoT apps are not hosted on-premises, and this Safeguard is out of scope.
6.4	Users	Protect	Require MFA for Remote Network Access	See [i.10]	●	●	●	N	The scope of this guide primarily focuses on IoT devices used within the enterprise.
6.5	Users	Protect	Require MFA for Administrative Access	See [i.10]	●	●	●	Y	To the extent practical in IoT, MFA should always be used, although this is not always supported on IoT. Standards such as the IETF Authentication and Authorization for Constrained Environments offer more robust solutions than traditional MFA [i.26].
6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	See [i.10]		●	●	N	Although an important Safeguard, IoT specific authentication systems are not commonplace.
6.7	Users	Protect	Centralize Access Control	See [i.10]		●	●	N	A majority of IoT devices do not allow for a centralized point of authentication. For instance, IoT devices utilizing a cloud platform will not allow enterprises to insert themselves into the authentication process.
6.8	Data	Protect	Define and Maintain Role-Based Access Control	See [i.10]			●	N	Most IoT devices do not provide role-based accounts.

4.3.7 CONTROL 07 Continuous Vulnerability Management

IoT Applicability

While vulnerability management is applicable to IoT devices, it is a much more difficult challenge when compared to traditional desktops, servers, or even mobile. Just as with other devices on a network, regularly scheduled vulnerability assessments should be conducted to determine non-secure configurations that lead to elevated threats to the enterprise. These security flaws should be remediated quickly, and the processes used for remediation should be fed back into the processes used for deployment new IoT devices.

IoT Challenges

Active vulnerability assessments of IoT devices in an operational environment may be dangerous to the health and proper functioning of the device. Improper vulnerability scans may lead to system instability or failure. Ideally, how the device will react when scanned is known by the IT administrator before the scan is initiated. As an alternative, passive vulnerability assessment can be a less intensive method to identify vulnerabilities identified without the risk of harming the IoT device and affecting other network operations. These assessments can be done manually or with automated tools sold by a third-party vendor. Although many IoT devices will be deployed internally, and not directly exposed to the internet, routine scanning for externally exposed assets is prudent. Tools exist that can detect externally exposed devices and help administrators either remove or properly configure them.

IoT Additional Discussion

Before putting an IoT device into operation, a process should be developed for managing IoT device vulnerabilities. This may be a subset of a larger vulnerability management plan, or dedicated to IoT. Different approaches may be needed for certain types of IoT devices, such as those residing outside the enterprise, on-site with clients, or functioning in a critical infrastructure sector. Topics for an IoT vulnerability management plan include: patch management, time to remediate, and disclosing issues with clients. For the subset of IoT devices that receive security patches from their vendor, they should be kept up-to-date. Outdated firmware often contains exploitable vulnerabilities that an attacker could leverage to access enterprise data.

A laboratory testing environment may be appropriate for regularly scheduled assessments against new threats and new IoT firmware configurations. Collaborative threat laboratories (e.g. sponsored by an Information Sharing & Analysis Center (ISAC) or other industry body) and IoT vendor laboratories may be the best venues for implementing this Control. As with other hardware and firmware vulnerabilities, these new vulnerabilities should also be evaluated against the enterprise's risk appetite to determine when a particular device or device class can no longer be supported on the network, or when it should be isolated.

Control 7: Continuous Vulnerability Management					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	See [i.10]	●	●	●	Y	Existing vulnerability management processes should include IoT devices, and include dedicated portions for different IoT use cases.
7.2	Applications	Respond	Establish and Maintain a Remediation Process	See [i.10]	●	●	●	Y	Vulnerability processes for IoT devices often involve updating firmware from the device manufacturer, and potentially a cellular radio if applicable. Any mobile applications used for IoT device management will also need to be updated.
7.3	Applications	Protect	Perform Automated Operating System Patch Management	See [i.10]	●	●	●	N	Many IoT devices cannot be updated via a centralized tool. If updates are available at all, devices generally need to be individually updated. It is often difficult to separate operating system level patches from the application providing the device's primary function.
7.4	Applications	Protect	Perform Automated Application Patch Management	See [i.10]	●	●	●	N	Many IoT devices cannot be updated via a centralized tool. If updates are available at all, devices generally need to be individually updated. It is often difficult to separate operating system level patches from the application providing the device's primary function.
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets	See [i.10]		●	●	Y	Enterprise IoT assets used internally should be scanned in an automated manner to the extent practical.
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets	See [i.10]		●	●	Y	Enterprise IoT assets used externally should be scanned in an automated manner to the extent practical.
7.7	Applications	Respond	Remediate Detected Vulnerabilities	See [i.10]		●	●	Y	Forcing platform updates at a specific time is not always possible, although some devices can be configured for automated firmware updates. This should lead to a timely update process. This is the best way to ensure vulnerabilities are remediated on IoT devices.

4.3.8 CONTROL 08 Audit Log Management

IoT Applicability

IoT device logs are structured in a variety of file formats because they are no uniform standards for storing and transferring IoT data. Some industries and use cases may have standards available. Administrators in these sectors should understand these formats in order to properly implement this Control.

Each device manufacturer is free to create their own format, making integrations from multiple vendors within the same network difficult. Furthermore, IoT devices may not be configured to log events; they may store logs locally on the device; or they may be sending them off to a local gateway or cloud platform. Enterprises should ensure that IoT devices create detailed logs and many IoT devices have this capability, but this capability needs to be verified before purchase. Additionally, a trusted method of extracting and parsing audit logs from relevant components should be available. However, this may prove challenging in some instances where OS and application logs are not enabled or available. To the degree possible, the default stance should always be to attempt to collect these logs.

IoT Challenges

Having logs from IoT devices is one measure of success but means little to an enterprise's cybersecurity posture if they are not being reviewed on a regular basis. Another challenging area related to IoT security is how to integrate large amounts of security data from diverse enterprise devices into an enterprise's Security Information and Event Management (SIEM) system. The creation of custom connectors should be investigated when IoT components do not provide standards-based log output. Just as important is a focus on how to make sense of the IoT log data when combined with standard network data captured by the SIEM. The establishment of rules that correlate this diverse data effectively will be an interesting challenge moving forward. Cloud-based analysis may be a potential solution to these challenges.

Developers may be concerned about writing logs too often to flash memory, which can potentially lead to excessive wear on the flash memory modules. This is an open problem, and developers should attempt to strike their own balance based on customer need.

IoT Additional Discussion

Legacy IoT systems are designed for reliable operations and rapid recovery. Accordingly, some of these systems include the ability to generate logs. Command and control subsystems may use alternative, out-of-band logging of activities that should be considered when assessing the implementation of this Control, or the need for separate, compensating controls.

Control 8: Audit Log Management					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	See [i.10]	●	●	●	Y	IT professionals should understand the types of logs available via their unique assembly of IoT devices, supporting infrastructure, and apps. The method of obtaining logs from each device type should be documented.
8.2	Network	Detect	Collect Audit Logs	See [i.10]	●	●	●	Y	If IoT device logs are created and available for export, they should be regularly extracted and reviewed.
8.3	Network	Protect	Ensure Adequate Audit Log Storage	See [i.10]	●	●	●	Y	This is particularly important for IoT devices with constrained memory storage. It is difficult to ascertain before a purchase if a device contains sufficient local storage capacity for detailed event logs. If sufficient storage is unavailable, old logs may be written over. Another solution is to send the logs off-device to a gateway or cloud platform.
8.4	Network	Protect	Standardize Time Synchronization	See [i.10]		●	●	Y	Developers of IoT devices may be able to design individual applications to utilize additional time sources, but this is an extremely uncommon feature.
8.5	Network	Detect	Collect Detailed Audit Logs	See [i.10]		●	●	Y	This is always a concern for any type of information system.
8.6	Network	Detect	Collect DNS Query Audit Logs	See [i.10]		●	●	N	This is a network-level mitigation, out of scope for IoT.
8.7	Network	Detect	Collect URL Request Audit Logs	See [i.10]		●	●	N	There is nothing specific to IoT within this Safeguard.
8.8	Devices	Detect	Collect Command-Line Audit Logs	See [i.10]		●	●	Y	Log management at scale can provide useful information about the state and health of fielded devices. This information should be stored and processed via a single resource.
8.9	Network	Detect	Centralize Audit Logs	See [i.10]		●	●	Y	IoT devices do not make log centralization easy. This should be done to the extent practical.
8.10	Network	Protect	Retain Audit Logs	See [i.10]		●	●	N	There is nothing specific to IoT within this Safeguard.
8.11	Network	Detect	Conduct Audit Log Reviews	See [i.10]		●	●	Y	Administrators and IT professionals should review audit logs for unexpected accesses to enterprise resources.
8.12	Data	Detect	Collect Service Provider Logs	See [i.10]			●	Y	If this information is available, it should be collected and analysed.

4.3.9 CONTROL 09 Email and Web Browser Protections

IoT Applicability

IoT devices generally do not use email or external web browser applications or interfaces. Some stand-alone IoT management systems may leverage standard web browser technologies for visualization and a common user experience. The majority of IoT devices will use email and browsers in a "headless" fashion.

IoT Challenges

Some devices will run a web server in order to support Representational State Transfer (RESTful) web services. Unfortunately, it is not always possible to apply hardening guidance such as the Benchmarks to IoT devices using web technologies. Embedded devices are commonly built without any way of modifying internal firmware.

IoT Additional Discussion

IT equipment that is used to transfer or bridge data between an IoT network and an IT corporate or other non-IoT operational network may incorporate email or web browser functionality. These applications should be protected according to best practice. In cases where web browser technologies are incorporated in stand-alone IoT networks, a risk analysis should be performed to address the need to update the applications when patches and new versions are released.

Control 9: Email and Web Browser Protections					Implementation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Framework Title**	**Framework Description**	**IG1**	**IG2**	**IG3**	**Included?**	**Justification**
9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	See [i.10]	●	●	●	Y	Although browsers and email clients should be kept up-to-date, it is difficult to do this for IoT devices. Enterprises should attempt to verify that updates are regularly applied to IoT devices.
9.2	Network	Protect	Use DNS Filtering Services	See [i.10]	●	●	●	N	In order for this mitigation to be put into place, it would have to be done at the network level.
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters	See [i.10]		●	●	Y	Network-based proxies, firewalls, and other proxies can be configured for IoT devices, or specifically support capabilities to filter IoT traffic. Content blockers can be developed for certain applications.
9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	See [i.10]		●	●	N	This is generally not possible with common IoT devices.
9.5	Network	Protect	Implement DMARC	See [i.10]		●	●	N	Although DMARC is an important Safeguard, DMARC is implemented in DNS and mail servers, and therefore not applicable to individual IoT devices.
9.6	Network	Protect	Block Unnecessary File Types	See [i.10]		●	●	N	This is generally not possible with common IoT devices.
9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections	See [i.10]			●	N	This is generally not possible with common IoT devices.

4.3.10 CONTROL 10 Malware Defences

IoT Applicability

Malware affects IoT devices in similar ways to other platforms, as seen with high-profile attacks utilizing Distributed Denial of Service (DDoS) and explored in greater detail in the paper *DDoS in the IoT: Mirai and Other Botnets* [i.27]. Both malware and exploits are now tailored to IoT devices and platforms, which highlights the need for a robust strategy to defend against malware and malicious code.

IoT Challenges

Given the limited processing ability and limited power capacity of many IoT components, host-based malware protections may consume too much processing capability and energy to work effectively, necessitating alternative protections. Using commercial, network-based malware detection systems (e.g. in-line monitoring) may not be feasible due to latency requirements or the use of non-IP protocols, but this is changing. IoT-specific network monitoring devices are beginning to be available for both enterprises and consumers. Continuous monitoring at corporate or other gateways through which IoT device information (updates and/or data) flows may be used to detect adversary malware or to correlate observed activity with known, legitimate, and/or planned activity.

IoT Additional Discussion

Traditional anti-malware techniques are not feasible on IoT devices. At the very least, preventing IoT devices from being publicly exposed to and facing the internet will act as a potential barrier. Segmenting IoT devices to their own dedicated network may be a prudent strategy if possible.

A primary IoT malware attack vector is via the firmware update process. Intelligent device purchasing and supply chain risk management can help to address the risk of IoT-based malware. Periodic validation of IoT device operation via alternative information channels (e.g. analog records, operational anomaly detection through long-term analytics) may be helpful but will require collection and long-term storage of what is normally perishable data.

In certain industries where availability is the overriding concern (e.g. healthcare, energy), IoT devices may be uniquely vulnerable to DDoS. Anti-malware tools and techniques should be properly regression-tested to ensure that availability and reliability of the system will not be adversely affected. Additionally, all anti-malware tools should be configured such that a false positive detection will not negatively impact the availability or reliability of any critical processes. The MUD framework can be leveraged here to allowlist specific actions IoT devices can take, and then be used to prevent those activities from taking place. Testing may need to occur whenever a change is made to the anti-malware firmware such as a configuration change, firmware hotfix, or repository update. It is important to understand the attack patterns used to affect IoT devices in the industry.

Another product category that can assist in defence against malware is threat intelligence focused towards IoT devices. These services review Tactics, Techniques, and Procedures (TTPs) and provide a risk rating or threat score to analysts based on behavior and other factors. Finally, allowlisting of firmware can provide malware protection by preventing malicious code from executing in the first place.

Control 10: Malware Defences					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	See [i.10]	●	●	●	Y	It can be difficult to find anti-malware products that also integrate with solutions already being used within an enterprise. On-device IoT malware solutions are not often a possible solution, but should be researched often as the IoT market is rapidly changing. Devices supporting the MUD Framework can be particularly useful in implanting this Control and applicable Safeguards.
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	See [i.10]	●	●	●	Y	Malware developers adapt to new defences and find new infection vectors for attacking IoT devices. This means that malware signatures change over time. Updating managed anti-malware software will keep the defences up-to-date against new threats.
10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	See [i.10]	●	●	●	N	IoT devices typically do not have these features enabled. If this is necessary, verification of these features in IoT devices should be conducted before purchase and implementation.
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	See [i.10]		●	●	N	IoT devices do not typically have physical ports for removable devices and cannot perform scanning activities.
10.5	Devices	Protect	Enable Anti-Exploitation Features	See [i.10]		●	●	Y	These are either enabled by default on the operating system or they are not. Unfortunately, IoT devices typically do not have these features enabled. If these important anti-exploit technologies are necessary, verification of these features in IoT devices should be conducted before purchase and implementation.
10.6	Devices	Protect	Centrally Manage Anti-Malware Software	See [i.10]		●	●	Y	Effective anti-malware IoT products that also integrate with solutions already being used within an enterprise are often hard to come by. Regardless of whether the solution is centrally managed or not, a plan for dealing with malware, including incident response, should be in place prior to the introduction of IoT.

Control 10: Malware Defences					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
10.7	Devices	Detect	Use Behavior-Based Anti-Malware Software	See [i.10]		●	●	Y	On-device IoT malware solutions utilizing behavior-based techniques are unlikely to be available. Network-based malware detection mechanisms using behavioral techniques are a more reasonable IoT solution.

4.3.11 CONTROL 11 Data Recovery

IoT Applicability

Many IoT devices may provide onboard storage for data and logs, though some IoT devices do not. Devices that store data may transfer it to dedicated network storage locations for near-term or permanent storage. This can be done periodically or in near real-time. When taking an inventory of the types of IoT devices to be used within an enterprise, it is important to understand whether data is at risk of being lost at any given point in the architecture and whether to devise a plan for ensuring that data can be recovered in case of component failure. The recovery of information stored on IoT management platforms is an important consideration and these systems should be incorporated into the enterprise implementation of Control 11.

IoT Challenges

Creating backups of IoT data can be very difficult as traditional backup strategies simply will not work. For instance, even simple utilities such as *rsync* will not be available and are therefore not a valid option. Native backup capabilities may be provided by the device manufacturer, and this functionality should be understood before purchase and implementation. Native capabilities will differ, and may automatically back up to the cloud or a phone, and enterprises should understand how back ups function before usage in the enterprise.

IoT Additional Discussion

When IoT message traffic is perishable and temporary, the value of data recovery is limited to maintenance actions. Data recovery capabilities may be required for operational data at consolidation and action points for compliance or maintenance purposes. IoT devices often maintain data until an online connection (e.g. via Bluetooth, LoRaWAN Wi-Fi, cellular, etc.) is established with a gateway application. In these instances, sensitive data may continue to be resident on the device and may require a recovery capability.

Enterprises should verify and review backup settings from the device manufacturer, including any associated service within the IoT ecosystem, to make sure the proper information is backed up. Proper authentication mechanisms should be in place to protect any enterprise data backed up to a cloud platform. IoT devices may also unintentionally back up information to any desktop environment they are connected to, or even gateways and mobile devices. The creation of these backups should be prevented unless specifically authorized by the enterprise.

Control 11: Data Recovery					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	See [i.10]	●	●	●	Y	Enterprises should document the processes used to back up and also recover enterprise information within IoT environments.
11.2	Data	Recover	Perform Automated Backups	See [i.10]	●	●	●	Y	Users should regularly back up enterprise IoT data to approved backup locations. This includes backing up monitoring and administration-oriented data, such as logs that are stored on a system separate from the IoT device. Automated backups are not always possible for IoT platforms, but effort should be expended to ensure it is properly set up when available.
11.3	Data	Protect	Protect Recovery Data	See [i.10]	●	●	●	Y	Data protection controls need to be in place for both on-premises and cloud-based backup solutions. Some cloud-based services will provide data protection automatically, but users and enterprises need to verify the mitigations in place before electing to use a service. Any removable media for the device, alongside desktop backups, also needs to be protected.
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	See [i.10]	●	●	●	Y	Ransomware and its related offshoots (e.g. destructive malware) typically perform malicious activities on the device itself. This includes preventing access to the device, yet it rarely affects third-party cloud storage providers.
11.5	Data	Recover	Test Data Recovery	See [i.10]		●	●	Y	Employees and administrators should regularly perform tests of accessing and restoring backed up data. Regular recovery exercises help the enterprise go through the motions of accessing and using backed up data.

4.3.12 CONTROL 12 Network Infrastructure Management

IoT Applicability

This Control is not directly applicable to IoT devices but is relevant for the security of certain types of IoT gateways (e.g. Small office, Home office (SoHo) routers used as IoT and LoRaWAN gateways) as well as for the secure usage of general network devices. Guidance on Wi-Fi security is provided by the Controls, but it applies to all computing devices and not necessarily IoT. When there is a plan to undertake a medium- to large-scale deployment of IoT devices within an enterprise, take the opportunity to review the configurations for firewalls, routers, and switches to ensure that additional vulnerabilities are not introduced through misconfiguration or poor network architecture.

IoT Challenges

Legacy IoT systems may favor proprietary byte-oriented protocols, but legacy systems that migrate to TCP/IP (e.g. Modbus TCP) are often fragile and insecure. The absence of commercially available network devices for legacy networks limits the value of this Control for those networks.

The Internet Engineering Task Force (IETF) specifies the Manufacturer Usage Description (MUD) standard, which allows IoT devices to advertise their capabilities via the local network [i.23]. Using MUD, IoT devices can solely transmit and receive information they need to properly operate. This can be enforced via context specific policies. Practical examples of how to use this technology can be found in this guide from the National Cybersecurity Center of Excellence [i.24].

IoT Additional Discussion

Newer IoT devices often use RESTful APIs that require supporting web services to be implemented securely. In addition, many IoT devices implement IPv6 communications and sometimes use protocols such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) to support the ability for constrained IoT devices to connect to the internet. The introduction of IPv6 opens a whole new set of security considerations across network devices for operation in a secure manner.

As discussed in other Controls within this guide, the use of segregation strategies is strongly recommended to keep IoT components operating in their own zones or on their own separate networks. In cases where there should be a connection point between an IoT segment and the corporate network, boundary defence mechanisms should be put in place. Firewalls, IDS, and IPS can provide assurance that a compromise of the less-trusted IoT network will have limited effect on the more secure corporate network.

Control 12: Network Infrastructure Management					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	See [i.10]	●	●	●	Y	IoT gateways will need to regularly receive firmware updates.
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	See [i.10]		●	●	Y	Network architecture may need to consider legacy IoT devices that may be insecure. IoT devices without authentication to use the device (e.g. smart speaker) may need to be on their own network without access to enterprise resources.
12.3	Network	Protect	Securely Manage Network Infrastructure	See [i.10]		●	●	Y	Network infrastructure associated with IoT devices needs to be managed in a secure manner.
12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)	See [i.10]		●	●	Y	Architecture diagrams should be created and kept up-to-date. This documentation should include all types of IoT devices.
12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	See [i.10]		●	●	N	If IoT devices support this functionality, it should be used, but this would be abnormal.
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols	See [i.10]		●	●	Y	IoT devices should be researched beforehand to understand if they are using secure communication protocols.
12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	See [i.10]		●	●	N	IoT devices do not contain this capability.
12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources For All Administrative Work	See [i.10]			●	Y	Many consider network segmentation for IoT devices a critical safeguard in the enterprise. This is especially true for IoT devices processing sensitive enterprise information.

4.3.13 CONTROL 13 Network Monitoring and Defence

IoT Applicability

This is a particularly important set of mitigations for IoT devices, and similar strategies intended for traditional network monitoring situations apply, with the exception of utilizing host-based solutions on IoT devices. Defences and mitigations, such as network monitoring tools, email security, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) alerts, and logging of network-based events are all important and should be utilized to the extent possible. These can be implemented in segmented networks where IoT devices are utilized and routed instead of through the trusted enterprise network. Filtering IoT network to the extent practical is worthwhile, as is the usage of Security Information and Event Management (SIEM).

IoT Challenges

IoT devices are increasingly being used in stand-alone enterprise scenarios or connected to cloud-based platforms. Full infrastructures dedicated to IoT may be needed that supports capture, processing, and analysis of data from IoT endpoints in the cloud. In addition, IoT platforms may share and collate information from many different enterprises. For cloud-based systems that support IoT, consider cloud security best practices, and move to a data-centric security approach to support the sharing of IoT data across many different organizations. On-premises hosting of IoT information should be utilized where possible, but this is rarely the case. ETSI TR 103 959 [i.28] offers additional guidance for securing cloud environments.

IoT Additional Discussion

In many instances, a decision will be made to place IoT devices outside of the trusted network boundary. Even with the few devices utilizing data-in-transit encryption with vetted algorithms and reasonable key sizes, certain types of traffic will be leaked. Examples of this type of information may include: diagnostic information about the device, OS traffic back and forth with the ecosystem provider, and wireless traffic using Wi-Fi, Bluetooth, LoRaWAN, and cellular networks. These types of information leaks allow passively sniffing malicious actors to fingerprint the device. Some devices may automatically attempt to access or connect to Wi-Fi networks to which they have previously been associated. Denylisting certain Service Set Identifiers (SSIDs) on devices, like those from major retailers and cafes, can help prevent an IoT device from accessing a rogue version of that network and sending sensitive enterprise data over it. Many enterprises will use a combination of network segmentation approaches for better vetted devices that provide critical enterprise functions.

Control 13: Network Monitoring and Defence					Implementation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Framework Title**	**Framework Description**	**IG1**	**IG2**	**IG3**	**Included?**	**Justification**
13.1	Network	Detect	Centralize Security Event Alerting	See [i.10]		●	●	Y	SIEMs can help to correlate security events occurring on IoT devices with mobile, server, network appliances, or other events within the enterprise network.
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution	See [i.10]		●	●	N	IoT devices are unlikely to support this capability as a host-based IDS cannot be installed onto an embedded device. Devices leveraging the MUD framework can implement this Safeguard.
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution	See [i.10]		●	●	Y	Enterprises can ensure that signatures and other information used by the IDS are IoT-specific, and that their IDS is "IoT aware". This Safeguard is better and more easily enforced when an IoT gateway is in use or when devices route traffic through the enterprise.
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments	See [i.10]		●	●	Y	Segmented IoT devices should remain that way, and unwanted traffic should be filtered and understood.
13.5	Devices	Protect	Manage Access Control for Remote Assets	See [i.10]		●	●	Y	Administrators should attempt to obtain some degree of control over the security and configuration of any IoT devices accessing an internal network.
13.6	Network	Detect	Collect Network Traffic Flow Logs	See [i.10]		●	●	Y	Network traffic flow logs associated with IoT devices should be regularly accessed and stored elsewhere in accordance with an enterprise's data retention policy.
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution	See [i.10]			●	N	IoT devices are unlikely to support this capability as a host-based IPS cannot be installed onto an embedded device.
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution	See [i.10]			●	Y	Enterprises can ensure that any relevant IPS is "IoT aware". This Safeguard is better and more easily enforced when an IoT gateway is in use or when devices route traffic through the enterprise.
13.9	Devices	Protect	Deploy Port-Level Access Control	See [i.10]			●	Y	It is unlikely that this will be possible for most IoT devices, but if the capability is available, it should be enabled. Note that IEEE 802.1x [i.29] does not work on many IoT devices that do not support supplicant software. Network-level authentication can cause reliability issues if not strictly maintained.
13.10	Network	Protect	Perform Application Layer Filtering	See [i.10]			●	N	Although this Safeguard is quite useful, it is not specific to IoT.
13.11	Network	Detect	Tune Security Event Alerting Thresholds	See [i.10]			●	Y	Customizing a SIEM's ruleset to accommodate IoT devices currently utilized by an enterprise is prudent.

4.3.14 CONTROL 14 Security Awareness and Skills Training

IoT Applicability

Administrators and any employees responsible for deploying and managing IoT devices should be trained on risks and threats specific to IoT devices and platforms. The deployment of IoT components brings with it new operational capabilities as well as new system and security management requirements. Security awareness training should be tailored to all employees regularly using these devices to prevent Unauthorized access of enterprise IoT devices and data.

IoT Challenges

Ensuring that administrators and employees understand the threats IoT devices pose to their networks can be a challenging task. Special notice should be provided regarding any connection of insecure legacy devices to enterprise networks that handle sensitive enterprise information. Consumer IoT devices are often cheap, easily available, and become ubiquitous in daily living. Employees may attempt to bring unapproved devices into the office or remote locations to use. This could include connecting enterprise systems to these devices, or connecting the IoT devices directly to the network. Employees need to understand the security policies surrounding these actions.

IoT Additional Discussion

Enterprises need to work to understand if a skills gap exists for current staff. If so, then there is a need to work towards identifying appropriate training to fill those gaps. This is not a one-time activity; as time goes on, new threats will emerge that staff will need to learn and understand the impacts on enterprise IoT devices.

IoT introduces new concepts that include a heavy focus on RF communications, with a range of purpose-built protocols. Security engineering teams should understand the intricate details of these protocols to configure devices in a secure manner. In many cases, IoT subsystems should also be integrated into the larger enterprise through cloud-based APIs. This requires that security engineering teams be well-versed in the cloud-based technologies that support IoT.

Legacy operators are beginning to integrate IoT into their networks. When migrating to remote operations or reporting remote situational awareness need to ensure their remote operators have the skills and training to address the additional risks of leveraging internet-facing IoT devices for their work.

Control 14: Security Awareness and Skills Training					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	See [i.10]	●	●	●	Y	A strategy should be developed to address and educate users on security concerns surrounding the use of IoT devices. Understanding the habits of employees using enterprise-approved IoT devices can help focus future cybersecurity awareness training. It can also be beneficial to analyse the list of IoT devices used in the enterprise and plan specific training for staff with administrative privileges for those IoT devices.
14.2	N/A	Protect	Train Workforce Members to Recognize Social Engineering Attacks	See [i.10]	●	●	●	Y	This Safeguard is not generally applicable to IoT devices but may apply for simpler automated home IoT devices where users should be aware of attempts to gain administrative access to the device through social engineering.
14.3	N/A	Protect	Train Workforce Members on Authentication Best Practices	See [i.10]	●	●	●	Y	Secure authentication is different on IoT platforms, and employees should know the security risks and implications of insecurely connecting IoT devices to corporate networks.
14.4	N/A	Protect	Train Workforce on Data Handling Best Practices	See [i.10]	●	●	●	Y	Users should understand what data is sensitive on their IoT devices and how to prevent commingling alongside personal information.
14.5	N/A	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	See [i.10]	●	●	●	Y	This can be tailored to IoT-specific needs, such as what can happen if an insecure IoT device is connected to an enterprise network, or insecure data storage in an associated cloud platform.
14.6	N/A	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	See [i.10]	●	●	●	Y	Employees can be trained on what successful attacks on IoT devices look like and to whom they should be reported.
14.7	N/A	Protect	Train Workforce on How to Identify and Report if their Enterprise Assets are Missing Security Updates	See [i.10]	●	●	●	Y	This Safeguard can be tailored to users learning how to ensure IoT devices are up-to-date.
14.8	N/A	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	See [i.10]	●	●	●	N	This Safeguard does not apply to IoT devices connected to enterprise networks.
14.9	N/A	Protect	Conduct Role-Specific Security Awareness and Skills Training	See [i.10]		●	●	Y	Role-specific awareness training should include an IoT component.

4.3.15 CONTROL 15 Service Provider Management

IoT Applicability

The primary service providers for IoT devices will include the provider of cloud-based services to support IoT devices. These platforms will most often provide device management, monitoring, and access to data.

IoT Challenges

Small to medium-sized businesses may be unable to ensure that these large companies implement many of the practices necessitated by the safeguards found within this Control. Monitoring the security posture of IoT cloud platform providers will often be infeasible from a technical standpoint, and contractual or legal assurances will be necessary. Before entering a Service Provider's ecosystem, it is a worthwhile activity to understand the authentication mechanisms available to customers. At the very least, multi-factor authentication should be supported, providing integration with whatever identity services the primary organization utilizes.

IoT Additional Discussion

This Control revolves around obtaining assurances from Service Providers as to their cybersecurity practices. Not all Service Providers will protect an enterprise's data in the same manner. Accordingly, a Service Provider's cybersecurity posture affects their ability to secure enterprise data entrusted to them. Obtaining ongoing information about a Service Provider's security posture will be difficult. Customer breach notifications or even mentions in the media of a breach are solid points of data about security posture. If an enterprise is regularly breached, that may be a sign to use another IoT platform.

Control 15: Service Provider Management					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
15.1	N/A	Identify	Establish and Maintain an Inventory of Service Providers	See [i.10]	●	●	●	Y	The primary service providers include the device manufacturer, cloud-platform provider, mobile app developer, and any integrated devices or services needed for enterprise operations.
15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy	See [i.10]		●	●	Y	Policies for working with service providers should address handling enterprise data generated by, and traditionally stored on, IoT devices. Updates to this policy may be necessary when major changes happen to IoT devices, such as the addition of new functions via a major OS update or changes to the cloud platform.
15.3	N/A	Identify	Classify Service Providers	See [i.10]		●	●	Y	The enterprise resources an IoT device can access, alongside the data its sensors generate, are prime candidates for classifying service providers.
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements	See [i.10]		●	●	Y	Service Providers offering IoT devices should adhere to the security requirements of the enterprise. Enterprise security requirements should be tailored to IoT.
15.5	N/A	Identify	Assess Service Providers	See [i.10]			●	Y	Obtaining evidence that an IoT service provider adheres to enterprise security should be done in a similar manner to other service providers leveraged by the enterprise.
15.6	Data	Detect	Monitor Service Providers	See [i.10]			●	Y	Monitoring IoT service providers should be done in a similar manner to other service providers leveraged by the enterprise.
15.7	Data	Protect	Securely Decommission Service Providers	See [i.10]			●	Y	Enterprises need to ensure IoT service providers are securely decommissioned, to remove any data saved in their system to include user accounts, passwords, and credentials.

4.3.16 CONTROL 16 Application Software Security

IoT Applicability

This Control can be applied in a few distinct ways as software security can apply to:

1) developing IoT devices;

2) deploying cloud-based applications that IoT devices utilize;

3) writing mobile or other applications that govern the usage of an IoT device; and

4) creating an application that integrates with a device in some way, such as leveraging an API.

This Control is not focused on the development and manufacturing of IoT devices and instead guides enterprises on their usage of IoT. Device controllers are also out of scope for this Control.

IoT Challenges

Most enterprises will not be able to access the source code used within IoT devices on their networks. This includes the associated mobile applications and cloud platforms. In many instances, those responsible for application security for IoT devices would have to perform analysis on compiled binaries pulled from the devices, which can be an arduous and time-consuming task. Mobile applications may be more easily acquired, but the analysis would not be directly on the source, which increases the time and resources needed to perform the analysis. However, this can still be a valuable effort. For instance, privileged credentials for accessing an IoT device have been found inside of its corresponding mobile application. Or, in another instance, credentials can be shared between distinct devices from the same manufacturer.

IoT Additional Discussion

Enterprises may look to receive some level of assurance that device manufacturers of IoT components practiced software assurance fundamentals when developing the firmware that provides logic for these devices. There will likely be a number of proprietary applications (e.g. cloud service, mobile application) that communicate with the IoT components and devices located throughout the enterprise. For IoT devices, enterprises should understand which security best practices were employed by the manufacturer and help to push vendors toward secure software development methodologies. This should also be a part of acquisition requirements and evaluation before purchase.

Software being developed by enterprises to connect to IoT components should follow the same secure development standards that the enterprise is already using for other internally developed applications. The Open Web Application Security Project (OWASP®) provides a wide variety of guidance for assessing and developing IoT devices [i.30], and is a powerful resource for IoT security.

Control 16: Application Software Security					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process	See [i.10]		●	●	Y	In the context of IoT, establishing a secure software development process is leveraging coding best practices from the OWASP® IoT Project.
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	See [i.10]		●	●	Y	A vulnerability disclosure policy is key for receiving reports of vulnerabilities in an enterprise's own software, and addressing them before they are able to be publicly exploited. Vulnerability disclosure policies should include IoT devices and apps, and procedures to quickly remedy vulnerabilities.
16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities	See [i.10]		●	●	Y	This is an important step to ensure that vulnerabilities of the same type do not repeatedly occur in a codebase.
16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components	See [i.10]		●	●	Y	Third-party libraries, frameworks, and other technologies leveraged by mobile app developers should be identified, understood, and inventoried.
16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components	See [i.10]		●	●	Y	Inventoried third-party IoT products and services should be regularly reviewed for support, and updated.
16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	See [i.10]		●	●	Y	Administrators and security professionals will benefit from rating mobile device vulnerabilities. The Common Vulnerability Scoring System (CVSS) [i.31] does not differentiate between system types and is applicable to IoT devices and their associated management systems.
16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure	See [i.10]		●	●	N	These templates are typically unavailable for IoT devices.
16.8	Applications	Protect	Separate Production and Non-Production Systems	See [i.10]		●	●	Y	Non-production systems should not be exposed to untrusted parties, as they commonly store sensitive data, but are often not hardened or running up-to-date software.
16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding	See [i.10]		●	●	Y	Classes and training materials are easily available online and in-person to educate developers on the common pitfalls of secure software development for IoT platforms.
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures	See [i.10]		●	●	Y	Classes and training materials are easily available online and in-person to educate developers on the common pitfalls of secure software development for mobile platforms.

Control 16: Application Software Security					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components	See [i.10]		●	●	Y	IoT developers should leverage vetted security technologies whenever possible in lieu of building their own. Examples include known hardware, firmware, and trusted cloud technologies.
16.12	Applications	Protect	Implement Code-Level Security Checks	See [i.10]			●	Y	Static and dynamic analysis tools dedicated to IoT devices are available.
16.13	Applications	Protect	Conduct Application Penetration Testing	See [i.10]			●	Y	Firms specializing in penetration testing can be hired.
16.14	Applications	Protect	Conduct Threat Modeling	See [i.10]			●	Y	Threat modeling should be conducted for IoT devices and associated infrastructure.

4.3.17 CONTROL 17 Incident Response Management

IoT Applicability

Traditional incident response guidance applies and can be tailored to IoT. This includes the need for planning, defining roles and responsibilities, and defining an escalation path. As with traditional systems, the need to identify, investigate, respond, and recover from incidents involving IoT devices is important. IoT brings unique aspects to the incident response process which can include working closely with the device manufacturer who likely administers the associated cloud platform.

IoT Challenges

There are often multiple types of compromise that could occur. For instance, devices with active network connections to enterprise systems could be accessed in an Unauthorized manner. In a different type of compromise, enterprise data generated by the IoT device and stored in an online cloud-platform may be improperly accessed. Then, that enterprise data may then be available for download by anyone. In both manners of compromise, response plans should be tailored to address the course of action to take when one or more IoT components are compromised. This should include considering the need to perform forensics on the compromised component as well as the need to quickly ensure that the device is taken offline to limit the spread of the incident. It should be noted that IoT forensics requires specialized knowledge to perform. When considering data forensics for IoT devices, there are a wealth of different types of data available to support the objective of the acquisition, be it eDiscovery, misuse, or evidence collection to support a criminal case.

IoT Additional Discussion

IoT systems are generally operational and come with a complete maintenance-oriented incident response and management subsystem of technology and business processes. Cybersecurity incident response and management controls should be integrated into these maintenance operations. Operations personnel and incident responders need to be trained on what unusual behavior looks like for an IoT device. As IoT extends to support new business processes, perform a mapping of IoT systems to those business processes. This will aid in determining the Continuity Of Operations Planning (COOP) approach to maintaining IoT operations. As with traditional incident response processes, this part of the response process should be tested or exercised regularly.

Control 17: Incident Response Management					Implementation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Framework Title**	**Framework Description**	**IG1**	**IG2**	**IG3**	**Included?**	**Justification**
17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	See [i.10]	●	●	●	Y	Appropriate staff-level and management personnel should be specifically appointed for IoT incident response.
17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	See [i.10]	●	●	●	Y	Information for specific individuals and external organizations should be maintained for whom should be contacted regarding IoT incidents.
17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	See [i.10]	●	●	●	Y	Standards for reporting IoT incidents should be put in place that are mandated across the enterprise. This should include time to report, types of anomalous events, and details of any relevant incident.
17.4	N/A	Respond	Establish and Maintain an Incident Response Process	See [i.10]		●	●	Y	Written plans for IoT breaches are key to IoT incident response.
17.5	N/A	Respond	Assign Key Roles and Responsibilities	See [i.10]		●	●	Y	Especially if an enterprise is supporting IoT devices, personnel should be dedicated to IoT.
17.6	N/A	Respond	Define Mechanisms for Communicating During Incident Response	See [i.10]		●	●	Y	Processes for reporting IoT incidents should be put in place that are mandated across the enterprise. This should include the time to report, types of anomalous events, and the details of any relevant IoT incident.
17.7	N/A	Recover	Conduct Routine Incident Response Exercises	See [i.10]		●	●	Y	IoT devices can be periodically assessed in order to test IoT incident response procedures. This also helps to keep the necessary individuals aware of the IoT procedures.
17.8	N/A	Recover	Conduct Post-Incident Reviews	See [i.10]		●	●	Y	Make sure to interview personnel involved in IoT incident response in order to ensure that all necessary actions were performed, and that procedures are updated to include any new areas not initially envisioned.
17.9	N/A	Recover	Establish and Maintain Security Incident Thresholds	See [i.10]			●	Y	Depending on their criticality to the enterprise, a security incident affecting IoT systems may be more or less important to the enterprise.

4.3.18 CONTROL 18 Penetration Testing

IoT Applicability

Using traditional penetration testing methods, to include identifying open ports, existing services, and vulnerable software versions may not necessarily apply to IoT. Legacy devices may need to be omitted from penetration testing activities, especially if they are supporting an important business function. Testing may bring them offline and unable to easily return to service without causing business or service interruption. IoT typically expands the threat model facing an organization in unique ways that sometimes cannot be easily rectified or mitigated.

IoT Challenges

Many IoT systems do not have mature IP stacks to scan. Errors in scanning may severely impact business operations. All such tests and scans should be tested thoroughly in a non-operational testbed (including architectural review or even code review if possible), preferably under simulated practical load-in operations. Strict rules of engagement should be applied that preclude any possibility of unintended, unexpected, or unwanted operational impact. A good example is a realistic, offline, threat-driven scenario. The usage of automated penetration testing tools with offline configurations can give a hint as to how the real environment will perform.

Penetration testers and red team members should pay extra care in securing authorization to perform vulnerability assessment and pen testing activities on cloud-based services supporting IoT devices and any mobile devices with an application supporting an IoT device. Specific user or service-level approval may be necessary, more than what is typically provided by the enterprise.

IoT Additional Discussion

Areas of focus for penetration testing could include sniffing wireless communications, reverse engineering firmware, and scanning for unknown services. The use of a test lab and devices for more thorough hardware examination is relevant to IoT. The IoT Penetration Testing Guide [i.32] can be a useful starting point to begin IoT penetration testing exercises. The use of IoT components within an enterprise should result in a tailoring of pen tests and red team exercises to focus specifically on methods to gain access to the network by leveraging weaknesses in the design, configuration, or deployment of those IoT components.

Control 18: Penetration Testing					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Framework Title	Framework Description	IG1	IG2	IG3	Included?	Justification
18.1	N/A	Identify	Establish and Maintain a Penetration Testing Program	See [i.10]		●	●	Y	A penetration testing program geared toward IoT will include any relevant IoT devices, applications, cloud services, and gateways.
18.2	Network	Identify	Perform Periodic External Penetration Tests	See [i.10]		●	●	Y	The frequency of testing can be difficult to determine, especially when multiple versions of an app can be pushed in a single day. This will be a decision decided by the enterprise in question.
18.3	Network	Protect	Remediate Penetration Test Findings	See [i.10]		●	●	Y	Penetration testing results applicable to IoT systems should be remediated.
18.4	Network	Protect	Validate Security Measures	See [i.10]			●	N	There is nothing specific to IoT devices in this Safeguard.
18.5	N/A	Identify	Perform Periodic Internal Penetration Tests	See [i.10]			●	Y	Internal testing teams should review the security of IoT devices and supporting infrastructure on a regular basis.

Annex A: Bibliography

- DDoS in the IoT: Mirai and Other Botnets
- ICS Cert
- ICS ISAC
- OWASP IoT Testing Guide

History

Document history		
V1.1.1	August 2016	Publication
V2.1.1	September 2018	Publication
V3.1.1	July 2023	Publication