Center for Internet Security®

CIS Controls

Internet of Things

Companion Guide

Acknowledgments

The Center for Internet Security, Inc. (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editor

Joshua M. Franklin, CIS

Contributors

Tony Krzyzewski, SAM for Compliance Ltd.
Maurice Turner, Alliance for Securing Democracy
Kathleen Moriarty, CIS
Robin Regnier, CIS

Contents

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions that collectively form a defense-in-depth approach and best practices that mitigate the most common attacks against systems and networks. The CIS 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 CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, transportation, education, government, defense, and others. While the CIS 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 CIS Controls.

The purpose of the CIS Controls Internet of Things Community is to develop best practices and guidance for implementing the CIS 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 can't 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 agreed upon 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*, 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*, 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* 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 upon 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 analyzing the CIS Controls in the context of IoT. For each of the 18 CIS Controls, the following information is provided in this document:

- **Applicability** – This assesses the degree to which a CIS Control functions or pertains to IoT.
- **Challenges** – These are unique issues that make implementing any of the relevant CIS 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 this 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 Revision 1.

Note that the CIS Implementation Groups (IGs) are a guideline to help enterprises determine a starting point for implementation of the CIS Controls. This guide does not re-group the Safeguards for IoT, and instead maintains the same prioritization used in the CIS Controls. Enterprises will, at times, find the need to implement CIS 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 CIS Safeguards regardless of IG.

Terminology

As noted earlier, there are many definitions of IoT. Below are basic descriptions of IoT components and terminology that we use 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.

Applicability Overview

● More than 60% of CIS Safeguards apply

● Between 1% and 60% of CIS Safeguards apply

● 0% of CIS Safeguards apply

CONTROL	CIS CONTROL 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 Defenses	●
11	Data Recovery	●
12	Network Infrastructure Management	●
13	Network Monitoring and Defense	●
14	Security Awareness and Skills Training	●
15	Service Provider Management	●
16	Application Software Security	●
17	Incident Response Management	●
18	Penetration Testing	●

CONTROL 01

Inventory and Control of Enterprise Assets

Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

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 must 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 perverse 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.

CIS Control 1: Inventory and Control of Enterprise Assets

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	CONTROL TITLE	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory**	Devices	Identify	●	●	●	Yes	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.
	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.							
1.2	**Address Unauthorized Assets**	Devices	Respond	●	●	●	Yes	Unknown IoT devices and gateways connected to enterprise networks and systems should be quickly investigated and removed.
	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.							
1.3	**Utilize an Active Discovery Tool**	Devices	Detect		●	●	Yes	Active discovery tools should be implemented to identify IoT devices, although some types of scans could leave devices in a nonfunctional 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.
	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.							
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory**	Devices	Identify		●	●	Yes	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.
	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.							
1.5	**Use a Passive Asset Discovery Tool**	Devices	Detect			●	No	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.
	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.							

CONTROL 02

Inventory and Control of Software Assets

Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

IoT Applicability

Network scanning and agent-based approaches are typical methods for software asset management. As mentioned in CIS 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 must 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 can't 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.

CIS Control 2: Inventory and Control of Software Assets

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	CONTROL TITLE	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
2.1	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	•	•	•	Yes	At minimum, a listing of the firmware versions associated with the IoT device can be noted. This should include firmware and platform versions.

CIS Control 2: Inventory and Control of Software Assets

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	CONTROL TITLE	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
2.2	**Ensure Authorized Software Is Currently Supported** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	•	•	•	Yes	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	**Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	•	•	•	No	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	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Applications	Detect		•	•	No	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	**Allowlist Authorized Software** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Applications	Protect		•	•	No	This capability is unavailable on most IoT devices, many of which will lack the processing power or security architecture to perform allowlisting.
2.6	**Allowlist Authorized Libraries** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc. files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	Applications	Protect		•	•	No	Allowlisting individual libraries is typically not available on IoT devices.
2.7	**Allowlist Authorized Scripts** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	Applications	Protect			•	No	Allowlisting individual scripts is typically not available on IoT devices.

CONTROL 03

Data Protection

Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

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 analyzed.

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's 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 life time of the device.

Protections must 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.

CIS Control 3: Data Protection

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
3.1	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify	●	●	●	Yes	The elements of the data management process mentioned in this Safeguard description can all apply to IoT. It's possible that these can be addressed as a subcomponent of an IoT Security Policy, or possibly addressed as part of Data Management.
3.2	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Data	Identify	●	●	●	Yes	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	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Data	Protect	●	●	●	Yes	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	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	Data	Protect	●	●	●	Yes	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	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Data	Protect	●	●	●	Yes	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	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include, Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Devices	Protect	●	●	●	No	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 of Constrained Application Protocol (OSCOAP) may be a useful solution in the near future.[1]
3.7	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●	Yes	Data classification decisions should be explicitly made for IoT data, to include data stored on, or downloaded from, their management platforms.

[1] https://tools.ietf.org/id/draft-ietf-core-object-security-04.html

CIS Control 3: Data Protection

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
3.8	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●	Yes	The enterprise should understand how sensitive data is transferred to and from IoT devices, apps, and cloud-based platforms.
3.9	**Encrypt Data on Removable Media** Encrypt data on removable media.	Data	Protect		●	●	Yes	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	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include, Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Data	Protect		●	●	Yes	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	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Data	Protect		●	●	Yes	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	**Segment Data Processing and Storage Based on Sensitivity** Segment data processing and storage, based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Network	Protect		●	●	Yes	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	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●	No	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	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●	Yes	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.

CONTROL 04

Secure Configuration of Enterprise Assets and Software

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

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 your 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) must 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 your 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.

CIS Control 4: Secure Configuration of Enterprise Assets and Software

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
4.1	**Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●	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	**Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●	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	**Configure Automatic Session Locking on Enterprise Assets** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	Users	Protect	●	●	●	N	This is not applicable to IoT devices as they are often headless.
4.4	**Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Devices	Protect	●	●	●	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	**Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Devices	Protect	●	●	●	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	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Network	Protect	●	●	●	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 OSCOAP.
4.7	**Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include, disabling default accounts or making them unusable.	Users	Protect	●	●	●	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.
4.8	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	Devices	Protect		●	●	N	IoT devices typically do not offer this level of feature granularity to IT administrators.

CIS Control 4: Secure Configuration of Enterprise Assets and Software

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
4.9	**Configure Trusted DNS Servers on Enterprise Assets** Configure trusted DNS servers on enterprise assets. Example implementations include, configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Devices	Protect		●	●	N	This is a network-level mitigation, out of scope for IoT.
4.10	**Enforce Automatic Device Lockout on Portable End-User Devices** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	Devices	Respond		●	●	N	IoT devices often will not have this feature available as they are often headless.
4.11	**Enforce Remote Wipe Capability on Portable End-User Devices** Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	Devices	Protect		●	●	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	**Separate Enterprise Workspaces on Mobile End-User Devices** Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Devices	Protect			●	N	This is not applicable to IoT devices.

CONTROL 05 Account Management

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

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 to 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. 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, and MFA solutions that might only be a password and PIN, which is not preferable to the first two options.

CIS Control 5: Account Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
5.1	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify	●	●	●	Yes	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	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Users	Protect	●	●	●	Yes	Administrative accounts for management, and any account used on the device, should use unique passwords.
5.3	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Respond	●	●	●	Yes	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	**Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged, account.	Users	Protect	●	●	●	Yes	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	**Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify		●	●	Yes	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	**Centralize Account Management** Centralize account management through a directory or identity service.	Users	Protect		●	●	Yes	Some IoT management technology can integrate with identity service providers, or may provide their own identity service. This is difficult to accomplish on IoT.

CONTROL 06

Access Management Control

Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

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 Management Control is meant to manage how a user accesses a device all the way through revoking access credentials and privileges. Thorough implementations of CIS Control 5 and Control 6 involve written policies addressing these areas before devices are provided to users. Although that's 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, athough 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 Security Information and Event Management (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.

CIS Control 6: Access Management Control

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
6.1	**Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Users	Protect	●	●	●	Yes	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	**Establish an Access Revoking Process** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Users	Protect	●	●	●	Yes	In addition to typical workstations and servers, administrators should define this process specifically for IoT devices, apps, gateways, and their management platforms.

CIS Control 6: Access Management Control

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
6.3	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Users	Protect	●	●	●	No	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	**Require MFA for Remote Network Access** Require MFA for remote network access.	Users	Protect	●	●	●	No	The scope of this guide primarily focuses on IoT devices used within the enterprise.
6.5	**Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Users	Protect	●	●	●	Yes	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.[1]
6.6	**Establish and Maintain an Inventory of Authentication and Authorization Systems** Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.	Users	Identify		●	●	No	Although an important Safeguard, IoT specific authentication systems are not commonplace.
6.7	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Users	Protect		●	●	No	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	**Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Data	Protect			●	No	Most IoT devices do not provide role-based accounts.

[1] https://datatracker.ietf.org/wg/ace/documents/

CONTROL 07

Continuous Vulnerability Management

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

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 of 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 like Shodan or Censys 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 must be isolated.

CIS Control 7: Continuous Vulnerability Management

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●	Yes	Existing vulnerability management processes should include IoT devices, and include dedicated portions for different IoT use cases.
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●	Yes	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.

CIS Control 7: Continuous Vulnerability Management

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●	No	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	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●	No	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	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Applications	Identify		●	●	Yes	Enterprise IoT assets used internally should be scanned in an automated manner to the extent practical.
7.6	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Applications	Identify		●	●	Yes	Enterprise IoT assets used externally should be scanned in an automated manner to the extent practical.
7.7	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Applications	Respond		●	●	Yes	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.

CONTROL 08

Audit Log Management

Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

IoT Applicability

IoT device logs are structured in a variety of file formats because there 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 must 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.

CIS Control 8: Audit Log Management

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
8.1	**Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●	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	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Network	Detect	●	●	●	Y	If IoT device logs are created and available for export, they should be regularly extracted and reviewed.
8.3	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Network	Protect	●	●	●	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	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	Network	Protect		●	●	Y	Developers of IoT devices may be able to design individual applications to utilize additional time sources, but this is an extremely uncommon feature.

CIS Control 8: Audit Log Management

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
8.5	**Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	Network	Detect		●	●	Y	This is always a concern for any type of information system.
8.6	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●	N	This is a network-level mitigation, out of scope for IoT.
8.7	**Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●	N	There is nothing specific to IoT within this Safeguard.
8.8	**Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	Devices	Detect		●	●	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	**Centralize Audit Logs** Centralize, to the extent possible, audit log collection, and retention across enterprise assets.	Network	Detect		●	●	Y	IoT devices do not make log centralization easy. This should be done to the extent practical.
8.10	**Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	Network	Protect		●	●	N	There is nothing specific to IoT within this Safeguard.
8.11	**Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	Network	Detect		●	●	Y	Administrators and IT professionals should review audit logs for unexpected accesses to enterprise resources.
8.12	**Collect Service Provider Logs** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events; data creation and disposal events; and user management events.	Data	Detect			●	Y	If this information is available, it should be collected and analyzed.

CONTROL 09 Email and Web Browser Protections

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

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 CIS 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.

CIS Control 09: Email and Web Browser Protections

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Applications	Protect	●	●	●	Yes	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	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●	Yes	In order for this mitigation to be put into place, it would have to be done at the network level.
9.3	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Network	Protect		●	●	Yes	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	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Applications	Protect		●	●	No	This is generally not possible with common IoT devices.
9.5	**Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		●	●	No	Although DMARC is an important Safeguard, DMARC is implemented in DNS and mail servers, and therefore not applicable to individual IoT devices.
9.6	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●	Yes	This is generally not possible with common IoT devices.
9.7	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●	No	This is generally not possible with common IoT devices.

CONTROL 10 Malware Defenses

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

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*. 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 your industry.

Another product category that can assist in defense 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.

CIS Control 10: Malware Defenses

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
10.1	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	Devices	Protect	●	●	●	Yes	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.

CIS Control 10: Malware Defenses

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
10.2	**Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	Devices	Protect	●	●	●	Yes	Malware developers adapt to new defenses 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 defenses up-to-date against new threats.
10.3	**Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	Devices	Protect	●	●	●	No	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	**Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	Devices	Detect		●	●	No	IoT devices do not typically have physical ports for removable devices and cannot perform scanning activities.
10.5	**Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	Devices	Protect		●	●	No	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	**Centrally Manage Anti-Malware Software** Centrally manage anti-malware software.	Devices	Protect		●	●	Yes	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.
10.7	**Use Behavior-Based Anti-Malware Software** Use behavior-based anti-malware software.	Devices	Detect		●	●	Yes	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.

CONTROL 11

Data Recovery

Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

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 your enterprise implementation of CIS 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 backups 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.

CIS Control 11: Data Recovery

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
11.1	**Establish and Maintain a Data Recovery Process** Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Recover	●	●	●	Yes	Enterprises should document the processes used to back up and also recover enterprise information within IoT environments.
11.2	**Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Data	Recover	●	●	●	Yes	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	**Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Data	Protect	●	●	●	Yes	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.

CIS Control 11: Data Recovery

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
11.4	**Establish and Maintain an Isolated Instance of Recovery Data** Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.	Data	Recover	●	●	●	Yes	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	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Data	Recover		●	●	Yes	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.

CONTROL 12

Network Infrastructure Management

Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

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 CIS 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.[1] Using MUD, IoT devices can solely transmit and receive information they need to

[1] https://datatracker.ietf.org/doc/rfc8520/

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.[1]

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 must be a connection point between an IoT segment and the corporate network, boundary defense mechanisms must 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.

CIS Control 12: Network Infrastructure Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
12.1	**Ensure Network Infrastructure is Up-to-Date** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Network	Protect	●	●	●	No	IoT gateways will need to regularly receive firmware updates.
12.2	**Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Network	Protect		●	●	No	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	**Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	Network	Protect		●	●	No	Network infrastructure associated with IoT devices needs to be managed in a secure manner.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf

CIS Control 12: Network Infrastructure Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
12.4	**Establish and Maintain Architecture Diagram(s)** Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Identify		●	●	No	Architecture diagrams should be created and kept up-to-date. This documentation should include all types of IoT devices.
12.5	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	Network	Protect		●	●	No	If IoT devices support this functionality, it should be used, but this would be abnormal.
12.6	**Use of Secure Network Management and Communication Protocols** Use secure network management and communication protocols (e.g. 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	Network	Protect		●	●	No	IoT devices must be researched beforehand to understand if they are using secure communication protocols.
12.7	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Devices	Protect		●	●	No	IoT devices do not contain this capability.
12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	Devices	Protect			●	No	Many consider network segmentation for IoT devices a critical safeguard in the enterprise. This is especially true for IoT devices processing sensitive enterprise information.

CONTROL 13

Network Monitoring and Defense

Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

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. Defenses 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. The *CIS Controls Cloud Companion Guide* 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.

CIS Control 13: Network Monitoring and Defense

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
13.1	**Centralize Security Event Alerting** Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts; a log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Network	Detect		●	●	Yes	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	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	Devices	Detect		●	●	Yes	IoT devices are unlikely to support this capability as you cannot install a host-based IDS onto an embedded device. Devices leveraging the MUD framework can implement this Safeguard.
13.3	**Deploy a Network Intrusion Detection Solution** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent Cloud Service Provider (CSP) service.	Network	Detect		●	●	No	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	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	Network	Protect		●	●	Yes	Segmented IoT devices should remain that way, and unwanted traffic should be filtered and understood.

CIS Control 13: Network Monitoring and Defense

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
13.5	**Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed; configuration compliance with the enterprise's secure configuration process; and ensuring the operating system and applications are up-to-date.	Devices	Protect		●	●	Yes	Administrators should attempt to obtain some degree of control over the security and configuration of any IoT devices accessing an internal network.
13.6	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Network	Detect		●	●	No	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	**Deploy a Host-Based Intrusion Prevention Solution** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	Devices	Protect			●	Yes	IoT devices are unlikely to support this capability as you cannot install a host-based IPS onto an embedded device.
13.8	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	Network	Protect			●	No	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	**Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	Devices	Protect			●	Yes	It is unlikely that this will be possible for most IoT devices, but if the capability is available, it should be enabled. Note that 802.1x 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	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	Network	Protect			●	No	Although this Safeguard is quite useful, it is not specific to IoT.
13.11	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	Network	Detect			●	No	Customizing a SIEM's ruleset to accommodate IoT devices currently utilized by an enterprise is prudent.

CONTROL 14

Security Awareness and Skills Training

Overview

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

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 isn't 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 must understand the intricate details of these protocols to configure devices in a secure manner. In many cases, IoT subsystems must 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, enterprises 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.

CIS Control 14: Security Awareness and Skills Training

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
14.1	**Establish and Maintain a Security Awareness Program** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Protect	●	●	●	Yes	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 analyze the list of IoT devices used in the enterprise and plan specific training for staff with administrative privileges for those IoT devices.
14.2	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	N/A	Protect	●	●	●	Yes	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	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	N/A	Protect	●	●	●	Yes	Secure authentication is different on IoT platforms, and employees should know the security risks and implications of insecurely N/Aconnecting IoT devices to corporate networks.
14.4	**Train Workforce on Data Handling Best Practices** Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	N/A	Protect	●	●	●	Yes	Users should understand what data is sensitive on their IoT devices and how to prevent commingling alongside personal information.

CIS Control 14: Security Awareness and Skills Training

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
14.5	**Train Workforce Members on Causes of Unintentional Data Exposure** Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	N/A	Protect	●	●	●	Yes	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	**Train Workforce Members on Recognizing and Reporting Security Incidents** Train workforce members to be able to recognize a potential incident and be able to report such an incident.	N/A	Protect	●	●	●	Yes	Employees can be trained on what successful attacks on IoT devices look like and to whom they should be reported.
14.7	**Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates** Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	N/A	Protect	●	●	●	Yes	This Safeguard can be tailored to users learning how to ensure IoT devices are up-to-date.
14.8	**Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks** Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	N/A	Protect	●	●	●	Yes	This Safeguard does not apply to IoT devices connected to enterprise networks.
14.9	**Conduct Role-Specific Security Awareness and Skills Training** Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	N/A	Protect		●	●	Yes	Role-specific awareness training should include an IoT component.

CONTROL

15 Service Provider Management

Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

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.

CIS Control 15: Service Provider Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers; include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.		Identify	●	●	●	Yes	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	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		Identify		●	●	Yes	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	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		Identify		●	●	Yes	The enterprise resources an IoT device can access, alongside the data its sensors generate, are prime candidates for classifying service providers.
15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements; security incident and/or data breach notification and response; data encryption requirements; and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		Protect		●	●	Yes	Service Providers offering IoT devices should adhere to the security requirements of the enterprise. Enterprise security requirements should be tailored to IoT.
15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaire, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.		Identify			●	Yes	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	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●	Yes	Monitoring IoT service providers should be done in a similar manner to other service providers leveraged by the enterprise.
15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●	Yes	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.

CONTROL **16**

Application Software Security

Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

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. Note that this guide 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, and is a powerful resource for IoT security.

CIS Control 16: Application Software Security

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
16.1	**Establish and Maintain a Secure Application Development Process** Establish and maintain a secure application development process. In the process, address such items as; secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect		●	●	Yes	In the context of IoT, establishing a secure software development process is leveraging coding best practices from the OWASP® IoT Project.
16.2	**Establish and Maintain a Process to Accept and Address Software Vulnerabilities** Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	Applications	Protect		●	●	Yes	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.

CIS Control 16: Application Software Security

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
16.3	**Perform Root Cause Analysis on Security Vulnerabilities** Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that creates vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	Applications	Protect		●	●	Yes	This is an important step to ensure that vulnerabilities of the same type don't repeatedly occur in a codebase.
16.4	**Establish and Manage an Inventory of Third-Party Software Components** Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	Applications	Protect		●	●	Yes	Third-party libraries, frameworks, and other technologies leveraged by mobile app developers should be identified, understood, and inventoried.
16.5	**Use Up-to-Date and Trusted Third-Party Software Components** Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Applications	Protect		●	●	Yes	Inventoried third-party IoT products and services should be regularly reviewed for support, and updated.
16.6	**Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities** Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.	Applications	Protect		●	●	Yes	Administrators and security professionals will benefit from rating mobile device vulnerabilities. The Common Vulnerability Scoring System (CVSS) does not differentiate between system types and is applicable to IoT devices and their associated management systems .
16.7	**Use Standard Hardening Configuration Templates for Application Infrastructure** Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	Applications	Protect		●	●	No	These templates are typically unavailable for IoT devices.
16.8	**Separate Production and Non-Production Systems** Maintain separate environments for production and non-production systems.	Applications	Protect		●	●	Yes	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	**Train Developers in Application Security Concepts and Secure Coding** Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	Applications	Protect		●	●	Yes	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.

CIS Control 16: Application Software Security

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
16.10	**Apply Secure Design Principles in Application Architectures** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.	Applications	Protect		●	●	Yes	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.
16.11	**Leverage Vetted Modules or Services for Application Security Components** Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.	Applications	Protect		●	●	Yes	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	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Applications	Protect			●	Yes	Static and dynamic analysis tools dedicated to IoT devices are available.
16.13	**Conduct Application Penetration Testing** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	Applications	Protect			●	Yes	Firms specializing in penetration testing can be hired.
16.14	**Conduct Threat Modeling** Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	Applications	Protect			●	Yes	Threat modeling should be conducted for IoT devices and associated infrastructure.

CONTROL 17

Incident Response Management

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

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. 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.

CIS Control 17: Incident Response Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
17.1	**Designate Personnel to Manage Incident Handling** Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Respond	●	●	●	Yes	Appropriate staff-level and management personnel should be specifically appointed for IoT incident response.
17.2	**Establish and Maintain Contact Information for Reporting Security Incidents** Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.		Respond	●	●	●	Yes	Information for specific individuals and external organizations should be maintained for whom should be contacted regarding IoT incidents.
17.3	**Establish and Maintain an Enterprise Process for Reporting Incidents** Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Respond	●	●	●	Yes	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	**Establish and Maintain an Incident Response Process** Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Respond		●	●	Yes	Written plans for IoT breaches are key to IoT incident response.

CIS Control 17: Incident Response Management

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
17.5	**Assign Key Roles and Responsibilities** Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Respond		●	●	Yes	Especially if an enterprise is supporting IoT devices, personnel should be dedicated to IoT.
17.6	**Define Mechanisms for Communicating During Incident Response** Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Respond		●	●	Yes	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	**Conduct Routine Incident Response Exercises** Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.		Recover		●	●	Yes	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	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.		Recover		●	●	Yes	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	**Establish and Maintain Security Incident Thresholds** Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		Recover			●	Yes	Depending on their criticality to the enterprise, a security incident affecting IoT systems may be more or less important to the enterprise.

CONTROL

18 Penetration Testing

Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

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 must 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 Attify IoT Penetration Testing Guide 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.

CIS Control 18: Penetration Testing

SAFEGUARD				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
18.1	**Establish and Maintain a Penetration Testing Program** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	N/A	Identify		●	●	Yes	A penetration testing program geared toward IoT will include any relevant IoT devices, applications, cloud services, and gateways.
18.2	**Perform Periodic External Penetration Tests** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Network	Identify		●	●	Yes	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	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Network	Protect		●	●	Yes	Penetration testing results applicable to IoT systems should be remediated.
18.4	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Network	Protect			●	No	There is nothing specific to IoT devices in this Safeguard.
18.5	**Perform Periodic Internal Penetration Tests** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	N/A	Identify			●	Yes	Internal testing teams should review the security of IoT devices and supporting infrastructure on a regular basis.

APPENDIX A

Acronyms and Abbreviations

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Network
ACK	Acknowledge
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
ARP	Address Resolution Protocol
CIS	Center for Internet Security
COOP	Continuity of Operations Planning
CSP	Cloud Service Provider
cTLS	compact Transport Layer Security
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
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
EDR	Endpoint Detection and Response
EMM	Enterprise Mobility Management
GDPR	General Data Protection Regulation
HART	Highway Addressable Remote Transducer
HIPAA	Health Insurance Portability and Accountability Act
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
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operating System
OSCOAP	Object Security of Constrained Application Protocol
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
PIN	Personal Identification Number
PKI	Public Key Infrastructure
REST(ful)	Representational State Transfer
RF	Radio Frequency
RFID	Radio Frequency Identifier
RSU	Roadside Unit
RTOS	Real-Time Operating System
SIEM	Security Information and Event Management
SP	Special Publication
SPF	Sender Policy Framework
SoHo	Small office home office
SSID	Service Set Identifier
SYN	Synchronization
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WPA2-PSK	Wi-Fi Protected Access 2 Pre-Shared Key

APPENDIX B

Links and Resources

- **CIS Controls** – https://www.cisecurity.org/controls/
- **CIS Controls Cloud Companion Guide** – https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/
- **CIS Controls Mobile Companion Guide** – https://www.cisecurity.org/white-papers/cis-controls-v8-mobile-companion-guide
- **Common Vulnerability Scoring System (CVSS)** – https://www.first.org/cvss/
- **DDoS in the IoT: Mirai and Other Botnets** – https://ieeexplore.ieee.org/abstract/document/7971869
- **ICS Cert** – https://ics-cert.us-cert.gov/
- **ICS ISAC** – http://ics-isac.org/blog/
- **Gartner's IT Glossary** – https://www.gartner.com/en/information-technology/glossary/internet-of-things
- **NIST SP 800-160 Revision 1** – https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
- **NIST SP 800-163 Revision 3** – https://pages.nist.gov/800-63-3
- **OWASP IoT Project** – https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- **OWASP IoT Testing Guide** – https://github.com/scriptingxss/owasp-fstm
- **The Internet of Things: An Overview** – https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf
- **Towards a Definition of the Internet of Things** – https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

APPENDIX C

Closing Notes

In this guide, we provide guidance on how to apply the security best practices found in CIS Controls Version 8 to IoT environments. The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, N.Y. 12061
518.266.3460
controlsinfo@cisecurity.org

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

To learn more, visit www.cisecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity