Establishing Essential Cyber Hygiene

Version 8.1

September 2024

CIS Center for Internet Security®
MS-ISAC® Multi-State Information Sharing & Analysis Center®
CIS Controls™

Acknowledgments

The Center for Internet Security® (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.

Editors

Valecia Stocchetti, CIS
Robin Regnier, CIS

Contributors

Josh Franklin, CIS
Tyler Scarlotta, CIS

Creative Commons

Contents

Introduction

In general, many cyber attacks can be attributed to a lack of good cyber hygiene. Simple enough, but there is an important idea in here. Study after study, and test after test gives us the same depressing result. Almost all successful attacks take advantage of conditions that could reasonably be described as "poor hygiene," including failure to patch known vulnerabilities, poor configuration management, and inefficient management of administrative privileges.

At CIS, we attribute these failures primarily to the complexity of modern systems management, as well as a noisy and confusing environment of technology, marketplace claims, and oversight/regulation ("The Fog of More"). Defenders are overwhelmed. Therefore, any large-scale security improvement program needs a way to bring focus and attention to the most effective and fundamental things that need to be done.

We do this at CIS by moving "cyber hygiene" from a notion or tagline into a campaign of specific actions, supported by a complementary market ecosystem of content, tools, training, and services. We codified our definition of "essential cyber hygiene" as consisting of the Safeguards found in Implementation Group 1 (IG1) of the CIS Critical Security Controls (CIS Controls). By defining IG1, we can then specify tools that can be put in place to implement the actions, measurements to track progress or maturity, and reporting that can be used to manage an enterprise improvement program. In today's environment of shared technology, linked by complex business relationships and hidden dependencies, this approach provides a specific way to negotiate "trust" and an "expectation" of security. (Are you a safe partner to bring into my supply chain? Can I count on this merchant to safely hold my financial information?) This approach is better than paper surveys or inconsistent interpretation of abstract security requirements.

IG1 is not just another list of good things to do; it is an *essential* set of steps that helps all enterprises deal with the most common types of attacks we see in real life. Our CIS Community Defense Model v2.0 provides the technical underpinning for that declaration.

The Center for Internet Security and its divisions, the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), are offering this guide as a resource to assist with the implementation of essential cyber hygiene, in alignment with the Nationwide Cybersecurity Review (NCSR) and National Institute of Standards and Technology® Cybersecurity Framework (NIST® CSF), by providing the tools, resources, and templates that are needed.

Why This Version?

CIS Controls version 8.1 (v8.1) is an iterative update to version 8.0. As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our design principles for this revision are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Clarity aligns with other major security frameworks to the extent practical, while preserving the unique features of the CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update.

How to Get Started

When tasked to implement a cybersecurity program, many enterprises ask “How do we get started?” In response, the Controls Community sorted the Safeguards in the CIS Controls into three Implementation Groups (IGs) based on their difficulty and cost to implement. IG1 is the group that is least costly and difficult to implement and are the Safeguards we assert that every enterprise should deploy. Applying all of the Safeguards listed in IG1 will help thwart general, non-targeted attacks and strengthen an enterprise’s security program. IG1 is *essential cyber hygiene* and represents a minimum standard of information security for all enterprises. We acknowledge that a listing of activities will not be the silver bullet for all security threats, but aim to provide activities for defending against common threats. For enterprises that face more sophisticated attacks or that must protect more critical data or systems, IG1 Safeguards provide the foundation for the other two Implementation Groups (IG2 and IG3).

Enterprises should first review this guide, which will provide an overview of each Safeguard in IG1 as well as why they are important to implement. Resources, tools, and policy templates that can be used to help facilitate implementation of these Safeguards are provided after the applicable Safeguard information, as well as in Appendix A and Appendix B of this guide. Enterprises can learn more about how they can gain access to multiple cybersecurity tools and resources through a CIS SecureSuite® Membership.[1] MS-ISAC and EI-ISAC membership. members can obtain a SecureSuite membership at no cost.

IG1 Safeguards: CIS Controls v8.1

The CIS Controls are a prioritized set of defensive actions aimed to protect enterprises from the most common attacks. They 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. Each CIS Control includes smaller actions, known as CIS Safeguards, which focus on measurable actions so you can more easily track your progress in applying effective protection against common attacks. There are 153 Safeguards in CIS Controls v8.1.

1 MS-ISAC and EI-ISAC members can obtain a SecureSuite membership at no cost.

As previously mentioned, in an effort to simplify and prioritize the process of effectively implementing the CIS Controls, CIS created three IGs—IG1, IG2, and IG3, as shown below. IGs are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards that they need to implement. IG1, "essential cyber hygiene," provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action, if warranted. Building upon IG1 is an additional set of Safeguards (IG2) for enterprises with more resources and expertise, but also greater risk exposure. Finally, the rest of the Safeguards make up IG3, for enterprises with the greatest risk exposure.

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153
TOTAL SAFEGUARDS

IG3 IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
SAFEGUARDS

IG2 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74
SAFEGUARDS

IG1 IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
SAFEGUARDS

CONTROL 1:

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.

Why It Matters

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them (CIS Control 3), and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

Safeguards

No.	Description	NIST CSF Security Function
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory**	Identify
	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, enterprise 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**	Respond
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Enterprise Asset Management Policy Template	The editable template can assist an enterprise in developing an enterprise asset management policy.	Control 1
CIS Asset Tracking Spreadsheet	Spreadsheet to help with asset and data inventory	1.1, 1.2
Nmap® Network Scanning	Tool used for reconnaissance and fingerprinting	1.1, 1.2
Zenmap	Nmap with a Graphical User Interface (GUI)	1.1, 1.2
Spiceworks®	IT inventory and asset management platform	1.1, 1.2
Open-AudIT®	Network device discovery and inventory auditing tool	1.1, 1.2
Microsoft® Configuration Manager	Windows® application within Microsoft® Endpoint Management used for configuration management	1.1, 1.2
NIST SP 1800-5	IT Asset Management	1.1, 1.2

CONTROL 2:

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.

Why It Matters

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software (CIS Control 7). However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Safeguards

No.	Description	NIST CSF Security Function
2.1	**Establish and Maintain a Software Inventory**	Identify
	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, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.	
2.2	**Ensure Authorized Software is Currently Supported**	Identify
	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.	

No.	Description	NIST CSF Security Function
2.3	**Address Unauthorized Software**	Respond
	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Software Asset Management Policy Template for CIS Control 2	The editable template can assist an enterprise in developing a software asset management policy	Control 2
CIS Asset Tracking Spreadsheet	Spreadsheet to help with asset and data inventory	2.1, 2.2, 2.3
Nmap® Network Scanning	Tool used for reconnaissance and fingerprinting	2.1, 2.2, 2.3
Zenmap	Nmap with a Graphical User Interface (GUI)	2.1, 2.2, 2.3
Spiceworks®	IT inventory and asset management platform	2.1, 2.2, 2.3
Open-AudIT®	Network device discovery and inventory auditing tool	2.1, 2.2, 2.3
Microsoft® Configuration Manager	Windows® application within Microsoft® Endpoint Management used for configuration management	2.1, 2.2, 2.3
NIST SP 1800-5	IT Asset Management	2.1, 2.2, 2.3
Supported Versions of Windows®	List of currently supported versions of Windows® 10 and 11	2.2
Endoflife.date	Community-maintained list of end-of-life software	2.2
Uninstall or Remove Apps and Programs in Windows® 10	Step-by-step on how to remove a program or application on Windows® 10	2.2
How to Uninstall Apps on your Mac	Step-by-step instructions on how to remove a program or application on macOS	2.2

CONTROL 3:

Data Protection

Overview

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

Why It Matters

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Safeguards

No.	Description	NIST CSF Security Function
3.1	**Establish and Maintain a Data Management Process**	Govern
	Establish and maintain a documented 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.	
3.2	**Establish and Maintain a Data Inventory**	Identify
	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.	
3.3	**Configure Data Access Control Lists**	Protect
	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.	
3.4	**Enforce Data Retention**	Protect
	Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.	

No.	Description	NIST CSF Security Function
3.5	**Securely Dispose of Data**	Protect
	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	
3.6	**Encrypt Data on End-User Devices**	Protect
	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Data Management Policy Template for CIS Control 3	The editable template can assist an enterprise in developing a data management policy	Control 3
CIS Asset Tracking Spreadsheet	Spreadsheet to help with asset and data inventory	3.2
Active Directory	Microsoft Windows® directory service for account management and access control	3.3, 3.4
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	3.3, 3.4
OpenLDAP	Open source implementation of the Lightweight Directory Access Protocol (LDAP)	3.3
Deploy Implementing Retention of Information on File Servers (Windows®)	How to set retention periods in Active Directory through Dynamic Access Control	3.4
Disk Wipe	Portable Windows® application to permanently delete data volumes	3.5
NIST SP 800-88 Rev. 1	Guides for Media Sanitization	3.5
VeraCrypt	On-the-fly encryption	3.6
Apple FileVault	Disk encryption for macOS	3.6
BitLocker	Built-in Windows® 10 utility used for full volume encryption	3.6

CONTROL 4:

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).

Why It Matters

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use, rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Safeguards

No.	Description	NIST CSF Security Function
4.1	**Establish and Maintain a Secure Configuration Process**	**Govern**
	Establish and maintain a documented 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.	
4.2	**Establish and Maintain a Secure Configuration Process for Network Infrastructure**	**Govern**
	Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	

No.	Description	NIST CSF Security Function
4.3	**Configure Automatic Session Locking on Enterprise Assets**	Protect
	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.	
4.4	**Implement and Manage a Firewall on Servers**	Protect
	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	
4.5	**Implement and Manage a Firewall on End-User Devices**	Protect
	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.	
4.6	**Securely Manage Enterprise Assets and Software**	Protect
	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) 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.	
4.7	**Manage Default Accounts on Enterprise Assets and Software**	Protect
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Secure Configuration Management Policy Template for CIS Control 4, 9, and 12	The editable template can assist an enterprise in developing a secure configuration management policy	Control 4
CIS Benchmarks™	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices	4.1, 4.2, 4.3, 4.4, 4.5, 4.7

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
CIS SecureSuite® Membership	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
CIS-CAT® Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
CIS Build Kits	ZIP files that contain a GPO for each profile within the corresponding CIS Benchmark	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
Active Directory	Microsoft Windows® directory service for account management and access control	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
OpenSCAP	Ecosystem providing many tools to assist with assessment, measurement, and enforcement of baselines	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
OpenVAS	Framework for vulnerability scanning and management	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
DISA STIGs	A set of configuration guides developed and maintained by the U.S. Department of Defense (DoD)	4.1, 4.2, 4.3, 4.4, 4.5, 4.7
RANCID	Monitors the configuration of network devices	4.2
OpenNAC	Network access control (NAC) solution	4.2
Zabbix	Monitoring tool for IT infrastructure	4.2

CONTROL 5:
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.

Why It Matters

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), using social engineering techniques to obtain a password, or using malware to capture passwords or tokens in memory or over the network. Defenders need to ensure that controls are in place to protect enterprise accounts, especially those with higher privileges.

Safeguards

No.	Description	NIST CSF Security Function
5.1	**Establish and Maintain an Inventory of Accounts**	Identify
	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service 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.	
5.2	**Use Unique Passwords**	Protect
	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.	
5.3	**Disable Dormant Accounts**	Protect
	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	
5.4	**Restrict Administrator Privileges to Dedicated Administrator Accounts**	Protect
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Account and Credential Management Policy Template for CIS Controls 5 and 6	The editable template can assist an enterprise in developing an account and credential management policy	Control 5
OpenLDAP	Open source implementation of the Lightweight Directory Access Protocol (LDAP)	5.1
Active Directory	Microsoft Windows® directory service for account management and access control	5.1, 5.3, 5.4
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	5.1, 5.3, 5.4
CIS Password Policy Guide	CIS Guidance for secure usage of passwords in an enterprise	5.2
KeePass	Password manager	5.2
Password Safe®	Simple and secure password management	5.2
Have I Been Pwnd	Public password data dumps	5.2
Specops Password Auditor	Active Directory password audit tool	5.2
NIST SP 800-63	Digital Identity Guidelines document suite, including NIST SP 800-63-3, NIST SP800-63A, NIST 800-63B, and NIST 800-63C	5.2, 5.4
CIS Benchmarks™	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices	5.4
CIS SecureSuite® Membership	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more	5.4
CIS-CAT® Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices	5.4
CIS Build Kits	ZIP files that contain a GPO for each profile within the corresponding CIS Benchmark	5.4

CONTROL 6:

Access Control Management

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.

Why It Matters

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Attackers will compromise any account that will grant them access to a network, especially administrator accounts that have elevated privileges. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Safeguards

No.	Description	NIST CSF Security Function
6.1	**Establish an Access Granting Process**	Govern
	Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.	
6.2	**Establish an Access Revoking Process**	Govern
	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.	
6.3	**Require MFA for Externally-Exposed Applications**	Protect
	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.	
6.4	**Require MFA for Remote Network Access**	Protect
	Require MFA for remote network access.	

No.	Description	NIST CSF Security Function
6.5	**Require MFA for Administrative Access**	Protect
	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Account and Credential Management Policy Template for CIS Controls 5 and 6	The editable template can assist an enterprise in developing an account and credential management policy	Control 6
Active Directory	Microsoft Windows® directory service for account management and access control	6.1, 6.2
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	6.1, 6.2
NIST SP 800-63	Digital Identity Guidelines document suite, including NIST SP 800-63-3, NIST SP800-63A, NIST 800-63B, and NIST 800-63C	6.1, 6.2, 6.3, 6.4, 6.5
Google Authenticator	Multi-step verification codes on your phone	6.3, 6.4, 6.5
Microsoft Authenticator	Multi-factor authentication application used for Microsoft® products	6.3, 6.4, 6.5
GCA Cybersecurity Toolkit for Small Business: Set Up 2FA on Your Accounts	Links to popular platforms providing instructions on how to turn on multi-factor authentication (MFA)	6.3, 6.4, 6.5
Two-Factor Authentication for Apple ID	How to set up two-factor authentication for your Apple ID	6.3, 6.4, 6.5

CONTROL 7:
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.

Why It Matters

Thousands of vulnerabilities are published each year, with several more that are unknown. Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Safeguards

No.	Description	NIST CSF Security Function
7.1	**Establish and Maintain a Vulnerability Management Process**	Govern
	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.	
7.2	**Establish and Maintain a Remediation Process**	Govern
	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	
7.3	**Perform Automated Operating System Patch Management**	Protect
	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	
7.4	**Perform Automated Application Patch Management**	Protect
	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Vulnerability Management Policy Template for CIS Control 7	The editable template can assist an enterprise in developing a data management policy	Control 7
CIS Benchmarks™	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices	7.1, 7.2, 7.3, 7.4
CIS SecureSuite® Membership	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more	7.1, 7.2, 7.3, 7.4
CIS-CAT® Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices	7.1, 7.2, 7.3, 7.4
CIS Build Kits	ZIP files that contain a GPO for each profile within the corresponding CIS Benchmark	7.1, 7.2, 7.3, 7.4
Active Directory	Microsoft Windows® directory service for account management and access control	7.1, 7.2, 7.3, 7.4
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	7.1, 7.2, 7.3, 7.4
OpenSCAP	Ecosystem providing many tools to assist with assessment, measurement, and enforcement of baselines	7.1, 7.2, 7.3, 7.4
OpenVAS	Framework for vulnerability scanning and management	7.1, 7.2, 7.3, 7.4
DISA STIGs	A set of configuration guides developed and maintained by the U.S. Department of Defense (DoD)	7.1, 7.2, 7.3, 7.4
Apple® Auto-update—iOS	Automatic updates for Apple® iOS devices	7.1, 7.2, 7.3, 7.4
Apple® Auto-update—macOS	Automatic updates for Apple® macOS devices	7.1, 7.2, 7.3, 7.4

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Auto-update Windows®	Automatic updates for Windows® devices	7.1, 7.2, 7.3, 7.4
Auto-update Microsoft® Office on macOS	Automatic updates for Microsoft® Office on macOS	7.1, 7.2, 7.3, 7.4
Auto-update Android™	Automatic updates for Android devices	7.1, 7.2, 7.3, 7.4
U.S. National Vulnerability Database (NVD)	Repository of standards based on vulnerability management data	7.1, 7.2, 7.3, 7.4
Nmap® Scripting Engine (NSE)	Tool used for vulnerability scanning, including identified Common Vulnerabilities and Exposures (CVEs)	7.1, 7.2, 7.3, 7.4
Lynis	Security audit tool used for system hardening	7.1, 7.2, 7.3, 7.4
NIST SP 800-40 Rev. 4	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	7.1, 7.2, 7.3, 7.4

CONTROL 8:

Audit Log Management

Overview

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

Why It Matters

Log collection and analysis is important for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. They know there's very little risk of being exposed through the audit logs if the logs are never analyzed. As a result, attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing. Logging records are critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack.

Safeguards

No.	Description	NIST CSF Security Function
8.1	**Establish and Maintain an Audit Log Management Process**	Govern
	Establish and maintain a documented 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.	
8.2	**Collect Audit Logs**	Detect
	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	
8.3	**Ensure Adequate Audit Log Storage**	Protect
	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Audit Log Management Policy Template for CIS Control 8	This template can assist an enterprise in developing an audit log management policy	Control 8
CIS Benchmarks™	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network device	8.1, 8.2, 8.3
CIS SecureSuite® Membership	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more	8.1, 8.2, 8.3
CIS-CAT® Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices	8.1, 8.2, 8.3
CIS Build Kits	ZIP files that contain a GPO for each profile within the corresponding CIS Benchmark	8.1, 8.2, 8.3
Active Directory	Microsoft Windows® directory service for account management and access control	8.1, 8.2, 8.3
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	8.1, 8.2, 8.3
OpenSCAP	Ecosystem providing many tools to assist with assessment, measurement, and enforcement of baselines	8.1, 8.2, 8.3
OpenVAS	Framework for vulnerability scanning and management	8.1, 8.2, 8.3
DISA STIGs	A set of configuration guides developed and maintained by the U.S. Department of Defense (DoD)	8.1, 8.2, 8.3
ELK Stack™	Acronym for three open source projects (Elasticsearch®, Logstash®, Kibana®) used for log aggregation	8.1, 8.2, 8.3
Syslog-ng®	Log management solution for Unix and Unix-like systems	8.1, 8.2, 8.3
AlienVault® OSSIM	Open-source security information and event management (SIEM) system	8.1, 8.2, 8.3

CONTROL 9:

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.

Why It Matters

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email, or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons. Defenders must ensure that browsers and email clients are kept up to date and that other activities, such as using DNS filtering services, are implemented to reduce the risk of a system communicating with a malicious domain.

Safeguards

No.	Description	NIST CSF Security Function
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients**	Protect
	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.	
9.2	**Use DNS Filtering Services**	Protect
	Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Secure Configuration Management Policy Template for CIS Control 4, 9, and 12	The editableCIS Control template can assist an enterprise in developing a secure configuration management policy	Control 9
U.S. National Vulnerability Database (NVD)	Repository of standards based on vulnerability management data	9.1
Nmap® Scripting Engine (NSE)	Tool used for vulnerability scanning, including identified Common Vulnerabilities and Exposures (CVEs)	9.1
Lynis	Security audit tool used for system hardening	9.1
NIST SP 800-40 Rev. 4	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	9.1
Comodo Dragon	Virtualized browser	9.1
NIST SP 800-177 Rev. 1	Trustworthy Email	9.1, 9.2
MS-ISAC® and EI-ISAC® Service: Malicious Domain Blocking and Reporting (MDBR)	MS-ISAC and EI-ISAC DNS filtering service that prevents IT systems from connecting to harmful web domains	9.2
Quad9®	Domain Name System (DNS) filtering service	9.2
OpenDNS®	Domain Name System (DNS) filtering service	9.2

CONTROL 10:

Malware Defenses

Overview

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

Why It Matters

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques. Malware defenses must be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

Safeguards

No.	Description	NIST CSF Security Function
10.1	**Deploy and Maintain Anti-Malware Software**	Detect
	Deploy and maintain anti-malware software on all enterprise assets.	
10.2	**Configure Automatic Anti-Malware Signature Updates**	Protect
	Configure automatic updates for anti-malware signature files on all enterprise assets.	
10.3	**Disable Autorun and Autoplay for Removable Media**	Protect
	Disable autorun and autoplay auto-execute functionality for removable media.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Malware Defense Policy Template for CIS Control 10	The editable template can assist an enterprise in developing a malware defense policy	Control 10
MS-ISAC® and EI-ISAC® Service: Malicious Code Analysis Platform (MCAP)	No-cost web-based sandbox to submit suspicious files to in a controlled and non-public fashion	10.1

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
European Institute for Computer Antivirus Research (EICAR) Anti-Virus Test File	File used to test anti-malware appliances	10.1, 10.2
ClamAV	Antimalware toolkit for UNIX	10.1, 10.2
Bitdefender® Antivirus Free	Antivirus for Android	10.1, 10.2
Windows® Defender Security Center	Anti-malware application built into Windows®	10.1, 10.2
Active Directory	Microsoft Windows® directory service for account management and access control	10.3
Local Group Policy Editor	Microsoft Management Console (MMC) snap-in used to configure or modify Group Policy settings with Group Policy Objects (GPOs)	10.3
OpenSCAP	Ecosystem providing many tools to assist with assessment, measurement, and enforcement of baselines	10.3
OpenVAS	Framework for vulnerability scanning and management	10.3
DISA STIGs	A set of configuration guides developed and maintained by the U.S. Department of Defense (DoD)	10.3
CIS Benchmarks™	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices	10.3
CIS SecureSuite® Membership	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more	10.3
CIS-CAT® Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices	10.3
CIS Build Kits	ZIP files that contain a GPO for each profile within the corresponding CIS Benchmark	10.3

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.

Why It Matters

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within IG1 of the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

Safeguards

No.	Description	NIST CSF Security Function
11.1	**Establish and Maintain a Data Recovery Process**	Govern
	Establish and maintain a documented 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.	
11.2	**Perform Automated Backups**	Recover
	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	
11.3	**Protect Recovery Data**	Protect
	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	
11.4	**Establish and Maintain an Isolated Instance of Recovery Data**	Recover
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Data Recovery Policy Template for CIS Control 11	The editable template can assist an enterprise in developing a data recovery policy	Control 11
DHS CISA & MS-ISAC® Joint Ransomware Guide	Ransomware best practices and recommendations based on operational insight from Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)	11.1, 11.2, 11.3, 11.4
VeraCrypt	On-the-fly encryption	11.1, 11.2, 11.3, 11.4
Microsoft® Backup and Restore	Built-in backup utility tool	11.1, 11.2, 11.3, 11.4
Microsoft® Volume Shadow Copy Service (VSS)	Tool to create backup copies or snapshots of files or volumes	11.1, 11.2, 11.3, 11.4
Bacula®	Network backup and recovery solution	11.1, 11.2, 11.3, 11.4
Amanda Network Backup	Backup tool	11.1, 11.2, 11.3, 11.4
Apple Time Machine	Built-in backup utility tool for macOS	11.1, 11.2, 11.3, 11.4
No More Ransom	Website to help victims of ransomware retrieve their data, report a crime, and more	11.1, 11.2, 11.3, 11.4
Clonezilla®	Disk imaging and cloning tool	11.1, 11.2, 11.3, 11.4
Redo™	Backup and disaster recovery tool	11.1, 11.2, 11.3, 11.4

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.

Why It Matters

Secure network infrastructure is an essential defense against attacks. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches. Default configurations for network devices are geared for ease-of-deployment and ease-of-use—not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unnecessary software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission. Ensuring that network infrastructure is kept up to date as well as establishing secure configurations (Safeguard 4.2) is an important line of defense to mitigate the risk of an attack.

Safeguards

No.	Description	NIST CSF Security Function
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.	**Protect**

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Secure Configuration Management Policy Template for CIS Control 4, 9, and 12	The editable template can assist an enterprise in developing a secure configuration management policy	Control 12
RANCID	Monitors the configuration of network devices	12.1
OpenNAC	Network access control (NAC) solution	12.1
Zabbix	Monitoring tool for IT infrastructure	12.1

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.

Why It Matters

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly. Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites. No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. An enterprise's training material should be reviewed and updated regularly. This will increase the culture of security and discourage risky workarounds.

Safeguards

No.	Description	NIST CSF Security Function
14.1	**Establish and Maintain a Security Awareness Program**	Govern
	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.	
14.2	**Train Workforce Members to Recognize Social Engineering Attacks**	Protect
	Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.	
14.3	**Train Workforce Members on Authentication Best Practices**	Protect
	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	

No.	Description	NIST CSF Security Function
14.4	**Train Workforce on Data Handling Best Practices**	Protect
	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.	
14.5	**Train Workforce Members on Causes of Unintentional Data Exposure**	Protect
	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.	
14.6	**Train Workforce Members on Recognizing and Reporting Security Incidents**	Protect
	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	
14.7	**Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates**	Protect
	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.	
14.8	**Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks**	Protect
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Security Awareness Skills Training Policy Template for CIS Control 14	The editable template can assist an enterprise in developing a security awareness skills training policy	Control 14
SANS: Ouch! Newsletters	Security awareness newsletter	14.1

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
SANS: Internet Storm Center®	Monitors the level of malicious activity on the internet	14.1
YouTube: Social Engineering Attacks (Professor Messer)	Educational videos	14.1, 14.2
NIST: You've Been Phished! videos	Educational videos	14.1, 14.2
Berkeley: The Phish Tank	Phishing examples	14.1, 14.2
MS-ISAC® Newsletter Subscription	Newsletters, advisories, and webinars on cybersecurity threats	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
MS-ISAC Cybersecurity Advisory Services Program (CASP)	Enhance an enterprise's cyber posture by providing cyber expertise to those that do not have it and cannot afford it.	Control 14
MS-ISAC® Cybersecurity Awareness Toolkit	Features educational materials designed to raise cybersecurity awareness. Digital materials are aggregated for your use	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
Federal Virtual Training Environment (FedVTE) Online Courses	Free online cybersecurity training to State, Local, Tribal, and Territorial (SLTT) governments	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
National Cyber Security Alliance (NCSA®)	Nonprofit promoting cybersecurity awareness and education	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
Center for Development of Security Excellence, Defense Counterintelligence and Security Agency	Provides assigned courses, including mandatory annual training, to DOD and other U.S. Government and defense industry personnel	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
YouTube: StaySafeOnline.org	Educational videos	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8

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.

Why It Matters

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions. There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise. Third-party providers serve as attractive targets for cyber-attacks due to the level of access they afford actors into the clients' networks and the ease with which actors can affect multiple victims by compromising one entity.

Safeguards

No.	Description	NIST CSF Security Function
15.1	**Establish and Maintain an Inventory of Service Providers**	Identify
	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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Service Provider Management Policy Template for CIS Control 15	The editable template can assist an enterprise in developing a service provider management policy	Control 15

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
CIS Companion Guide—Establishing Essential Cyber Hygiene Through a Managed Service Provider (MSP)	Guideline questionnaire to ensure that the enterprise's essential cyber hygiene needs are met by their MSP	15.1
FedRAMP	Standardized approach to security and risk assessment for cloud technologies and federal agencies	15.1

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.

Why It Matters

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

Safeguards

No.	Description	NIST CSF Security Function
17.1	**Designate Personnel to Manage Incident Handling**	Respond
	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, service providers, or a hybrid approach. If using a service provider, 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.	
17.2	**Establish and Maintain Contact Information for Reporting Security Incidents**	Govern
	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service 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.	

No.	Description	NIST CSF Security Function
17.3	**Establish and Maintain an Enterprise Process for Reporting Incidents**	Govern
	Establish and maintain an documented 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.	

Tools and Resources

Tool/Resource Name	Description	Control (#)/ Safeguard (#.#)
Incident Response Policy Template for CIS Control 17	The editable template can assist an enterprise in developing an incident response policy	Control 17
MS-ISAC Cybersecurity Enhancement and Incident Response	To aid SLTT entities in effectively implementing an incident response plan, serving as a resource for enhancing their cybersecurity programs.	17.1, 17.2, 17.3
MS-ISAC® and EI-ISAC® Service: Cyber Incident Response Team (CIRT)	SLTT governments can report incidents to the MS-ISAC Call 866-787-4722 or email soc@cisecurity.org for assistance from the MS-ISAC/EI-ISAC Security Operations Center (SOC) and Cyber Incident Response Team (CIRT)	17.1, 17.2, 17.3
NIST SP 800-61 Rev. 2	Computer Security Incident Handling Guide	17.1, 17.2, 17.3
NIST SP 800-184	Guide for Cybersecurity Event Recovery	17.1, 17.2, 17.3
Guide for Cybersecurity Incident Recovery	Provides strategic guidance for planning, developing, testing, and improvement of recovery planning following a cybersecurity incident.	17.1, 17.2, 17.3

Conclusion

IG1 (essential cyber hygiene) is a foundational set of cyber defense Safeguards that every enterprise (especially those with limited resources or expertise) should apply to guard against the most common attacks, and represents a minimum standard of information security for all enterprises. Essential cyber hygiene is the on-ramp to the CIS Controls. From there, enterprises may find that they need to implement higher-level CIS Safeguards, such as those found in IG2 and IG3, as their risk profiles increase. Each IG builds upon the previous one: IG2 includes IG1, and IG3 includes all CIS Safeguards in IG1 and IG2.

This guide aims to provide essential cyber hygiene activities from the CIS Controls, as well as their relationship to the NIST Cybersecurity Framework. Implementation of these practices through an MS-ISAC and EI-ISAC membership, a SecureSuite Membership, and other additional tools and resources will lead to a more formalized cybersecurity program to defend against common threats.

APPENDIX A:

CIS Controls Policy Templates

For our SLTT Community, the CIS Controls Policy Templates are also available within the CIS Workbench Platform within the CIS Controls – Policy Template Community.

Acceptable Use Policy Template for the CIS Controls	The editable template can assist an enterprise in developing acceptable use for the CIS Controls.	Download
Enterprise Asset Management Policy Template for CIS Control 1	The editable template can assist an enterprise in developing an enterprise asset management policy.	Download
Software Asset Management Policy Template for CIS Control 2	This template can assist an enterprise in developing a software asset management policy.	Download
Data Management Policy Template for CIS Control 3	The editable template can assist an enterprise in developing a data management policy.	Download
Secure Configuration Management Policy Template for CIS Control 4, 9, and 12	The editable template can assist an enterprise in developing a secure configuration management policy.	Download
Account and Credential Management Policy Template for CIS Controls 5 and 6	The editable template can assist an enterprise in developing an account and credential management policy.	Download
Vulnerability Management Policy Template for CIS Control 7	The editable template can assist an enterprise in developing a data management policy.	Download
Audit Log Management Policy Template for CIS Control 8	The editable template can assist an enterprise in developing an audit log management policy.	Download

Malware Defense Policy Template for CIS Control 10	The editable template can assist an enterprise in developing a malware defense policy.	Download
Data Recovery Policy Template for CIS Control 11	The editable template can assist an enterprise in developing a data recovery policy.	Download
Security Awareness Skills Training Policy Template for CIS Control 14	The editable template can assist an enterprise in developing a security awareness skills training policy.	Download
Service Provider Management Policy Template for CIS Control 15	The editable template can assist an enterprise in developing a service provider management policy.	Download
Incident Response Policy Template for CIS Control 17	The editable template can assist an enterprise in developing an incident response policy.	Download

APPENDIX B:

Other Policy Templates

The MS-ISAC provides (Courtesy of the State of New York and the State of California) the following policy templates that can be customized and used as an outline of an organizational policy, with additional details to be added by the enterprise.

Identify

- Acceptable Use of Information Technology Resources Policy
- Access Control Policy
- Account Management/Access Control Standard
- Identification and Authentication Policy
- Information Security Policy
- Security Assessment and Authorization Policy
- Security Awareness and Training Policy
- System and Communications Protection Policy
- Information Classification Standard
- Information Security Risk Management Standard
- Risk Assessment Policy
- Systems and Services Acquisition Policy
- Monitoring Vendor Performance & Compliance Policy Template
- Vendor Acquisition & Selection Policy Template
- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Access Control Policy

Protect

- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Policy
- Identification and Authentication Policy
- Sanitization Secure Disposal Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard
- 802.11 Wireless Network Security Standard
- Mobile Device Security
- System and Information Integrity Policy
- Acceptable Use of Information Technology Resources Policy
- Information Security Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy
- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Encryption Standard
- Incident Response Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard
- Remote Access Standard
- Security Logging Standard

Detect

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard
- Encryption Standard
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard
- Security Assessment and Authorization Policy
- Secure Coding Standard
- Computer Security Threat Response Policy
- Incident Response Policy
- Cyber Incident Response Standard

Respond

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Planning Policy

Recover

- Computer Security Threat Response Policy
- Contingency Planning Policy
- Cyber Incident Response Standard
- Incident Response Policy

APPENDIX C:

IG1 Safeguards Covered by CIS, MS-ISAC, and EI-ISAC[1] Tools

Safeguard(s)	Subject	Tool(s)
Asset Management		
1.1	**Enterprise Asset Management Policy/Process**	CIS Controls Enterprise Asset Management Policy Template
1.1, 1.2, 2.1, 2.2, 2.3, 9.1, 12.1	**Enterprise and Software Asset Management Tool**	CIS Controls Asset Tracking Spreadsheet
2.1	**Software Asset Management Policy/Process**	CIS Controls Software Asset Management Policy Template
15.1	**Service Provider Management Tool**	
Data Management		
3.1	**Data Management Policy/Process**	CIS Controls Data Management Policy Template
3.2	**Data Management Tool**	CIS Controls Asset Tracking Spreadsheet
3.5	**Data Disposal Tool**	
3.6	**Encryption Tool**	

1 Multi-State Information Sharing and Analysis Center® (MS-ISAC), Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC)

Safeguard(s)	Subject	Tool(s)
Secure Configurations		
4.1, 4.2	**Secure Configuration Policy/Process**	CIS Controls Secure Configuration Management Policy Template
4.1, 4.2, 4.3, 4.6, 4.7, 5.4, 10.3	**Configuration Management Tool**	CIS Benchmarks™ (PDF versions) – Best Practice Guidance CIS-CAT®[2] Lite – Tool for implementing Best Practice Guidance CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs[3] CIS Hardened Images®
4.4, 4.5	**Firewall**	CIS Benchmarks™ (PDF versions) – Best Practice Guidance CIS-CAT® Lite – Tool for implementing Best Practice Guidance CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs - Best Practice Guidance CIS Hardened Images®
Account and Access Control Management		
6.1, 6.2	**Account and Credential Management Policy/Process**	CIS Controls Account and Credential Management Policy Template
3.3, 3.4, 5.1, 5.3, 5.4	**Identity and Access Management Tool**	
5.2	**Password Management Tool**	CIS Controls Password Policy Guidance
6.3, 6.4, 6.5	**Multi-Factor Authentication Tool**	

2 CIS Configuration Assessment Tool (CIS-CAT)
3 U.S. State, Local, Tribal, and Territorial (SLTT) government entities

Safeguard(s)	Subject	Tool(s)
Vulnerability Management		
7.1	**Vulnerability/Patch Management Policy/Process**	CIS Controls Vulnerability Management Policy Template
7.2, 7.3, 7.4	**Vulnerability/Patch Management Tool**	
Log Management		
8.1	**Log Management Policy/Process**	CIS Controls Audit Log Management Policy Template
8.2, 8.3	**Log Management Tool**	CIS Benchmarks™ (PDF versions) – Best Practice Guidance CIS-CAT® Lite – Tool for implementing Best Practice Guidance CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs CIS Hardened Images®
Malware Defense		
10.1, 10.2	**Anti-Malware Software**	CIS Endpoint Security Services (ESS) - SLTTs only
9.2	**DNS Service/Server**	MS-ISAC® and EI-ISAC® Service: Malicious Domain Blocking and Reporting (MDBR) service – MS-/EI-ISAC Members only
Data Recovery		
11.1	**Data Recovery Policy/Process**	CIS Controls Data Recovery Policy Template
11.2, 11.3, 11.4	**Data Backup and Recovery Tool**	

Safeguard(s)	Subject	Tool(s)
Security Training		
14.1	**Security Training and Awareness Policy/Process**	CIS Controls Security Awareness Skills Training Policy Template
14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8	**Security Training and Awareness Tool(s)**	MS-ISAC® Advisories/Newsletter Subscription – Available to everyone MS-ISAC® Cybersecurity Awareness Toolkit – SLTTs only
Incident Response		
17.1, 17.2, 17.3	**Incident Response Planning**	MS-ISAC® and EI-ISAC® Service: Cyber Incident Response Team (CIRT) - SLTTs only

APPENDIX D:
Links and Resources

CIS Critical Security Controls (CIS Controls) v8.1:	Learn more about the CIS Controls, including how to get started, why each Control is critical, procedures and tools to use during implementation, and a complete listing of Safeguards for each Control.
CIS Controls v8.1 Mapping to NIST CSF	To provide the connection between the CIS Controls v8.1 and NIST CSF frameworks.
CIS Controls Assessment Specification	Provides an understanding of what should be measured in order to verify that the Safeguards are properly implemented.
CIS Controls Navigator	Learn more about the Controls and Safeguards and see how they map to other security standards (e.g., CMMC, NIST SP 800-53 Rev. 5, PCI DSS, MITRE ATT&CK).
CIS Community Defense Model (CDM) v2.0	A guide published by CIS that leverages the open availability of comprehensive summaries of attacks and security incidents, and the industry-endorsed ecosystem that is developing around the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Model.
CIS Risk Assessment Method (CIS RAM) v2.1	An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.
CIS SecureSuite Membership:	No-cost membership to SLTTs, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more.
CIS Benchmarks	Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices.
CIS-CAT Pro	Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices.
The Cost of Cyber Defense: CIS Controls IG1	CIS has published *The Cost of Cyber Defense: Implementation Group 1 (IG1),* to help you answer these questions: which protections to start with; which tools will be needed to implement those protections; and how much an implementation will cost.

Reasonable Cybersecurity	A guide on how the CIS Controls can be implemented prescriptively and in a manner that affords all those who use and rely on the technology ecosystem the ability to assess whether reasonable cybersecurity measures were taken.
CIS Build Kits	ZIP files that contain a Group Policy Object (GPO) for each profile within the corresponding CIS Benchmark.
CIS Hardened Images®	Virtual machine images securely pre-configured to the CIS Benchmarks.
CIS WorkBench	Get involved in one of our many communities.
CIS Password Policy Guide	CIS Guidance for secure usage of passwords in an enterprise.
MS-ISAC Membership	Free for all 50 states, the District of Columbia, U.S. territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the U.S.
EI-ISAC Membership	Free for all SLTT government organizations that support the elections officials of the U.S., and associations thereof.
MS-ISAC Cybersecurity Resources Guide	Mapping of various resources to NIST CSF.
Malicious Domain Blocking and Reporting	MS-ISAC and EI-ISAC DNS filtering service that prevents IT systems from connecting to harmful web domains.
Nationwide Cybersecurity Review (NCSR)	No-cost, anonymous, annual self-assessment designed to evaluate cybersecurity maturity.
NIST CSF Policy Template Guide	Resource to assist with the application and advancement of cybersecurity policies.
No-Cost and Fee-Based Listing of MS-ISAC/EI-ISAC Services	Overview of available services. Contact info@cisecurity.org for more information.
Tabletop Exercises	Tabletop exercises are meant to help organizations consider different risk scenarios and prepare for potential cyber threats.

APPENDIX E:

Acronyms and Abbreviations

CIRT	Cyber Incident Response Team
CIS	Center for Internet Security
CIS-CAT	CIS Configuration Assessment Tool
CIS CDM	CIS Community Defense Model
CIS CSAT	CIS Controls Self Assessment Tool
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CVEs	Common Vulnerabilities and Exposures
DNS	Domain Name System
DoD:	U.S. Department of Defense
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
FedVTE	Federal Virtual Training Environment
GPO	Group Policy Object
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IG	Implementation Group
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
IoT	Internet of Things
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MCAP	Malicious Code Analysis Platform
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MMC	Microsoft Management Console
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSP	Managed Service Provider
NAC	Network Access Control
NaaS	Network as a Service
NCSR	Nationwide Cybersecurity Review
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
PCI DSS	Payment Card Industry Data Security Standard
SBP	Security Best Practices
SOC	Security Operations Center
SLTT	State, Local, Tribal, and Territorial governments
SP	Special Publication
SSH	Secure Shell
Telnet	Teletype Network Protocol
URL	Uniform Resource Locator

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.

CIS Center for Internet Security®

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