

First Steps Within a Cybersecurity Program

Contents

Introduction	1
High Priority Cybersecurity Actions	2
1 Inventory and Control of Hardware Assets	2
2 Inventory and Control of Software Assets	2
3 Continuous Vulnerability Management	3
4 Controlled Use of Administrative Privileges	4
5 Configuration for Hardware and Software on Mobile Devices, Laptops, and Servers	4
6 Maintenance, Monitoring, and Analysis of Audit Logs	5
Appendix	6

Introduction

This guide provides high priority actions that can be implemented to establish and improve an organization's cybersecurity program. The following guidance utilizes resources from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the CIS Security Best Practices (SBP) team, including information within the CIS Controls. Alignment to the NIST Cybersecurity Framework (CSF) is also included.

We acknowledge a listing of activities will not be the end-all for security threats, but aim to provide activities to consider for mitigating common threats. The information in this document is meant to guide a user and does not reflect any specific organization. Each organization will have its own priorities and business needs that should be considered while consulting this guide.

Additional information on CIS, MS-ISAC, and the NIST CSF are located in the Appendix of this guide. This includes details on the MS-ISAC's no-cost Nationwide Cybersecurity Review (NCSR), which allows an organization to assess their cybersecurity maturity within the areas described in this guide and access additional valuable resources.

High Priority Cybersecurity Actions

1

Inventory and Control of Hardware Assets

Overview: Managing hardware devices on the network ensures that only authorized devices gain access and unauthorized or unmanaged devices are kept out.

Why It Matters: Attackers scan for devices that are not properly configured with security updates, including employees' personal devices, to gain internal access and pivot to the next victims.

Main Points and Actions to Take:

- Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
- Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

Related Resources:

- **No-Cost Resource:** CIS Asset Tracking Spreadsheet: <https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/>
- **Open Source Tools:** Nmap, OpenVAS

Related NIST Cybersecurity Framework (CSF) Categories:

- Identify – Asset Management (ID.AM)
- Protect – Identity Management & Access Control (PR.AC)
- Protect – Data Security (PR.DS)
- Detect – Security Continuous Monitoring (DE.CM)

2

Inventory and Control of Software Assets

Overview: Like hardware management, there should be inventory, tracking, and correction of all software installed to prevent unauthorized or unmanaged software to install or execute.

Why It Matters: Seemingly innocuous software can be vulnerable to exploitation. Furthermore, sometimes it can come pre-equipped with tools for an attacker to compromise the system, which in turn can become a launchpad to compromise others.

Main Points and Actions to Take:

- Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

- Utilize application allow-listing technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

Related Resources:

- **No-Cost Resource:** CIS Asset Tracking Spreadsheet: <https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/>
- **Open Source Tools:** [SnipeIT](#), [Quad9](#)

Related NIST Cybersecurity Framework (CSF) Categories:

- Identify – Asset Management (ID.AM)
- Protect – Data Security (PR.DS)
- Detect – Security Continuous Monitoring (DE.CM)

3 Continuous Vulnerability Management

Overview: Rather than a quarterly check or semi-regular one, continuously identifying vulnerabilities and remediation shrinks the window of opportunity for attackers.

Why It Matters: Attackers take advantage of gaps between new knowledge and remediation, and institutions that do not constantly scan for vulnerabilities and proactively face weaknesses are far more likely to suffer system compromise.

Main Points and Actions to Take:

- Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
- Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

Related Resources:

- **No-Cost Services:** [MS-ISAC & EI-ISAC Membership](#), [CIS SecureSuite Membership](#), [CIS-CAT Pro Configuration Assessor](#)
- **Open Source Tools:** [Nmap](#), [OpenVAS](#)

Related NIST Cybersecurity Framework (CSF) Categories:

- Identify – Risk Assessment (ID.RA)
- Protect – Information Protection Processes and Procedures (PR.IP)
- Detect – Security Continuous Monitoring (DE.CM)
- Respond – Mitigation (RS.MI)

4 Controlled Use of Administrative Privileges

Overview: Special administrative privileges on computers, networks, and applications must be tracked, controlled, and corrected if misused.

Why It Matters: This is the primary method for attackers to infiltrate a target. Often a privileged user is fooled into opening a malicious email or attachment. Similarly, if passwords are loosely or widely distributed, they can more easily be guessed or cracked.

Main Points and Actions to Take:

- Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
- Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

Related Resources:

- **Open Source Tools:** [Quad9](#), [OpenNAC](#), [PacketFence](#)

Related NIST Cybersecurity Framework (CSF) Categories:

- Protect – Identity Management & Access Control (PR.AC)
- Protect – Protective Technologies (PR.PT)
- Detect – Security Continuous Monitoring (DE.CM)

5 Configuration for Hardware and Software on Mobile Devices, Laptops, and Servers

Overview: Active implementation and management of the security configuration and controls process prevents attackers from exploiting vulnerable services and settings.

Why It Matters: Most default configurations are geared toward convenience, not security. And even if the default is strong, it can decay over time and create openings.

Main Points and Actions to Take:

- Maintain documented, standard security configuration standards for all authorized operating systems and software.
- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Related Resources:

- **No-Cost Services:** [MS-ISAC & EI-ISAC Membership](#), [CIS SecureSuite Membership](#), [CIS-CAT Pro Configuration Assessor](#)
- **Open Source Tool:** [DMARC](#)

Related NIST Cybersecurity Framework (CSF) Categories:

- Protect – Information Protection Processes and Procedures (PR.IP)
 - Detect – Security Continuous Monitoring (DE.CM)
-

6

Maintenance, Monitoring, and Analysis of Audit Logs

Overview: Collection, management, and analysis of audit logs can help detect, understand, or recover from an attack.

Why It Matters: Without comprehensive documentation and analysis of logs, an attack may go unnoticed and cause damage.

Main Points and Actions to Take:

- Ensure that local logging has been enabled on all systems and networking devices.
- Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

Related Resources:

- **CIS Service:** [Albert Network Monitoring](#)
- **Open Source Tool:** [OSSIM](#)

Related NIST Cybersecurity Framework (CSF) Categories:

- Detect – Anomalies and Events (DE.AE)
- Protect – Data Security (PR.DS)
- Protect – Protective Technologies (PR.PT)
- Respond – Analysis (RS.AN)

Appendix

CIS Resources:

- CIS Security Best Practices (SBP) Cyber Hygiene Article: <https://www.cisecurity.org/media-mention/practice-cyber-hygiene-with-6-basic-cis-controls/>
- CIS Controls Information: <https://www.cisecurity.org/controls/>
- CIS SecureSuite Information: <https://www.cisecurity.org/cis-securesuite/>

MS-ISAC & NIST Resources:

- Multi-State Information Sharing and Analysis Center (MS-ISAC) Overview: <https://www.cisecurity.org/isac/>
- National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF): <https://www.nist.gov/cyberframework>
- NIST CSF Policy Template Guide Published by MS-ISAC: <https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf>.
- Policy development can help formalize cybersecurity activities within an organization.

Nationwide Cybersecurity Review (NCSR):

For information on the Nationwide Cybersecurity Review (NCSR), please visit the following page: <https://www.cisecurity.org/ms-isac/services/ncsr/>. This no-cost self-assessment from the MS-ISAC allows a State, Local, Tribal, or Territory level organization to measure the gaps and capabilities of their cybersecurity program. The NCSR assessment utilizes the activities from the NIST Cybersecurity Framework (CSF) as its question set. The following reporting templates display the alignment between an organization's NCSR results, the NIST CSF, the activities within this guide, and additional resources:

NCSR & CIS Controls:

- [CIS Controls Version 7.1 – NCSR Results/NIST CSF Mapping Template](#)

NCSR & Cybersecurity Resources:

- [Cybersecurity Resources Guide – NCSR Results/NIST CSF Mapping Template](#)

Contact Information:




For MS-ISAC specific questions, please contact info@msisac.org.

For CIS specific questions, please utilize the following contact form: <https://enroll.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 CISecurity.org or follow us on Twitter: @CISecurity.

-  cisecurity.org
-  info@cisecurity.org
-  518-266-3460
-  [Center for Internet Security](https://www.linkedin.com/company/center-for-internet-security)
-  [@CISecurity](https://twitter.com/CISecurity)
-  [CenterforIntSec](https://www.facebook.com/CenterforIntSec)
-  [TheCISecurity](https://www.youtube.com/channel/UC...)
-  [cisecurity](https://www.instagram.com/cisecurity)