Elections Infrastructure ISAC®

Essential Guide to Election Security

Release 1.0.0

Center for Internet Security

Aug 30, 2022

INTRODUCTION

CHAPTER

ONE

THE ESSENTIAL GUIDE TO ELECTION SECURITY

Want to skip straight to the action?

- Determine your *maturity level*
- See *best practices* for your maturity

To first learn more, read on…

1.1 A Best Practices Resource for Election Professionals

The Center for Internet Security (*CIS*) has developed this Essential Guide to Election Security to serve as a first-stop resource for election officials to learn about best practices in election security. This can aid the process of building a program designed to meet individual needs and abilities of any given election office.

This Guide considers the wide range of technical capabilities and resource availability among the many thousands of election offices in the United States. While providing guidance for all organizational maturities, it emphasizes guidance for small jurisdictions without extensive cybersecurity resources available to them. The most important practices are included for those jurisdictions, with opportunities to ramp up as they mature.

It's an online guide and is continually updated, though readers can easily export it as a PDF. Read more about this Guide and how it came to be in our *about this guide* appendix.

1.2 Who should use this Guide?

This Guide helps election officials and their staffs understand their organizational cybersecurity readiness and take steps to improve. It is for jurisdictions of all of sizes and types, though which best practices apply to you will depend on several factors, including, but not limited to:

- The type of jurisdiction (state vs. county vs. municipality),
- The structure of election administration in a given state (top-down vs. bottom-up),
- The types of election equipment owned, and
- How IT responsibilities are shared with other functions in the jurisdiction, such as when IT is shared with the rest of the county.

Election technology providers and other stakeholders will also find much of the information useful as they consider how their work impacts outcomes in election administration and security.

1.3 How do I use this Guide?

The Guide is organized into several sections:

1. An introduction,
2. A description of *maturities* and how they are used in the document,
3. A set of *best practices* for organizations to implement, and
4. Additional references, tools, and related information in *appendices*.

You can get more detailed information this Guide and how to use it in our *how to*.

1.4 Identifying Your Organization's Security Lead

Regardless of the size of your office, one of the most effective steps to increasing your security posture is identifying someone who you'll hold accountable for making progress in examining your current maturity status, maintaining existing security processes, implementing best practices, and taking additional steps towards increasing your security posture.

This individual should own and maintain the process of improving your cybersecurity posture, whether you use this Guide to do so or any other resource. Accountability matters!

1.5 A Little Encouragement Before You Start

Many elections officials may not consider themselves security or IT professionals. This Guide takes this into consideration. In addition to implementing the best practices for your maturity, we encourage you to read through the entire Guide. It can provide you an understanding of the types of actions you may want to take as you continually improve your cybersecurity posture.

If you find yourself not understanding something, please reach out to the EI-ISAC elections team at elections@cisecurity.org and trusted partners and peers at the federal, state, and local levels for guidance and support.

This Guide was made possible through support from the Democracy Fund. The content of this Guide is the sole responsibility of CIS and may not reflect the views of its funders.

CHAPTER

TWO

MATURITIES

2.1 The Purpose of Maturities

Not all election offices have the same experience, resources, or needs. States and territories vary from a few thousand residents to tens of millions, counties and municipalities from a few dozen residents to more than ten million. The differences in populations-served result in widely varying tax bases, staffing levels, number and type of IT and physical assets, and more. Correspondingly, different election offices will implement different best practices at different times.

While an election office should implement best practices that best fit its needs, establishing maturities provides rough contours around these differences. By defining maturities, the EI-ISAC can provide a starting point that any given office can implement or use to tailor its approach.

2.2 Maturities in the Essential Guide

This section will help election officials determine their current maturity. This Guide defines three levels to reflect an organization's capabilities in managing cybersecurity risk. The maturities closely align to the three *CIS Controls* Implementation Groups (IGs), with important differences based on the nature of and risks associated with election administration. You can learn more about the CIS Controls and its IGs in the *CIS Controls* best practice.

The three maturities are:

1. Level 1: The organization responds to threats when presented to them or when attacked but has little capacity to predict, foresee, or model attacks.
2. Level 2: The organization focuses on deploying tools to stay ahead of threats and attempts to implement lessons learned. Some staff and contractors may specialize in cybersecurity but generally don't have specialized domains within cybersecurity.
3. Level 3: The organization assesses its risks and employs experts in the different facets of cybersecurity—e.g., risk management, penetration testing, application security.

2.3 Using the Maturity Levels

The next page will provide questions that can help guide you to one of the three maturities. Use it as a starting point and adjust as needed.

Each best practice has tailored guidance for each maturity, ranging from simple guidance and (usually free) tools for the Level 1 maturity to enterprise-driven and sophisticated guidance and tools for the Level 3 maturity.

CHAPTER

THREE

DETERMINE MATURITY

This section provides some general characteristics for each of the three maturities. Read through them, determine your current maturity, and use that maturity throughout the Guide to choose your implementation strategy.

If you've already implemented the guidance in a best practice for your overall maturity, consider leveling up to the next maturity for that best practice. It's all part of the process of continual improvement.

3.1 Level 1 Maturity

An organization is likely at a Level 1 maturity if most of the following statements apply:

1. You have no dedicated cybersecurity staff, though you may contract for IT staff or share an IT security resource with other governmental functions, such as a county recorder.
2. While cybersecurity matters to you, you most often consider it in terms of keeping systems operational and not about detailed threats.
3. You have not undergone a formal cybersecurity assessment, like the National Cybersecurity Review (*NCSR*). This is more than just automated scanning, but a full expert assessment.
4. You do not have current continuity of operations or disaster recovery plans or have rarely tested them.
5. You receive cybersecurity guidance and alerts from external sources, but have difficulty understanding or knowing how to apply them within your organization.
6. You don't have a thorough incident response plan, don't exercise it regularly, or don't feel confident in what to do when an incident occurs.

3.2 Level 2 Maturity

Your organization is likely at a Level 2 maturity if most of the following statements apply:

1. You have dedicated resources to manage and protect IT infrastructure.
2. You have already implemented basic cybersecurity measures, like Implementation Group 1 from the CIS Controls, the appropriate cybersecurity profile from the *NIST CSF*, or equivalent control sets.
3. When you receive cybersecurity alerts and directives, you generally know how to mitigate the risk.
4. You actively seek formal guidance for improving your cybersecurity posture.
5. You understand the threats facing your organization and other organizations similar to yours.
6. You track assets and conduct regular backups with at least one copy stored offline.

7. You respond to threat and risk assessments by developing and executing on plans of action and milestones (POAMs).

3.3 Level 3 Maturity

Your organization is likely at a Level 3 maturity if most of the following statements apply:

1. You have dedicated personnel with expertise in specific cybersecurity domains.
2. You have resources that specialize in different aspects of cybersecurity, such as penetration testing or application security.
3. You conduct regular cybersecurity assessments, have after-action plans, and track progress against those plans.
4. You conduct vulnerability management, including scanning for vulnerabilities, paying attention to threat intelligence, and creating prioritized lists for tackling vulnerabilities.
5. You have the ability to detect minor events and anomalous behavior, preventing major disruptions.
6. You leverage technology to help defend against nation-state threat actors and zero-day attacks.
7. You deploy tools to address major areas of cybersecurity defense, such as network monitoring, endpoint protection, and application firewalls.

3.4 What to do with your maturity?

Based on your maturity, you can begin implementation based on the guidance for that maturity within each best practice. If you find that guidance isn't what you expected, consider moving up or down in maturity. If you are at the Level 2 or Level 3 maturity, take the time to review best practices and recommendations from the earlier maturity(ies) to make sure that you've covered everything that makes sense for you.

All organizations are different with unique combinations of skills and resources. Election offices should tailor these implementation programs to make sense in the context of their respective capabilities and responsibilities, keeping in mind that the ultimate goal is not to fill in checkboxes but to develop effective and continually improving risk mitigation strategies.

CHAPTER

FOUR

PRIORITIZING BEST PRACTICES

No one wants to suffer a cybersecurity incident. The intent to protect networks is universal, but resource limitations leave many organizations facing perhaps the most difficult question in all of cybersecurity: What do I do next?

This section prioritizes best practices by mapping each maturity level to the priority best practices that should be implemented by an election office at that maturity level.

4.1 Level 1 Maturity

If you are at the Level 1 maturity, your first goal should be to commit to incrementally improving your maturity. This is about setting simple goals: complete one simple task a week, implement one best practice a month, and set aside a minimum set of resources dedicated to cybersecurity every quarter. Whatever helps you make progress.

4.1.1 Level 1 Maturity Baseline Priorities

The following is the list of priority actions at the Level 1 maturity. If you are at the Level 1 maturity, we recommend starting with these to establish a baseline of cyber hygiene.

Actions

1. Download and complete the *worksheets* for Level 1 maturity baseline. There are ten worksheets, all in one downloadable file.
    - Together, these fulfill all of the Level 1 baseline priorities. In the table below, the left column is the name of a Level 1 maturity worksheet described *here*. On that page you can download one file with all ten worksheets. The middle column gives the relevant best practice in this Guide for the worksheet tab, and the right columns lists the actions within that best practice that are fulfilled by completing the worksheet tab.

Worksheet	Best Practice (Actions from the Best Practice Adressed by the Worksheet)
• Hardware Inventory • Software Inventory • Data Inventory • Service Provider Inventory • Account Inventory	*Asset Management* (Action #1)
Asset Protection	• *Encrypt Data At Rest* (All Actions) • *Managing Infrastructure* (Actions #1 and #2)
Account Security	*User Management* (All Actions under User Recommendations)
Backup & Recovery	*Backups* (Action #1)
Incident Response	*Incident Response* (Actions #1 and #4)
Cyber Education	*Building and Managing Staff* (Actions #2 and #3)

While the needed effort can vary greatly depending on the size of your office and number of assets (computers, software, etc.), each *worksheet* is built to take no more than four hours the first time around and as little as 15 minutes each subsequent time. A suggestion: set aside time to do one a week until you've got them all done; then they're easy to repeat.

4.1.2 Level 1 Maturity Election Priorities

In addition to the above, you should be implementing some measures of particular importance to the election community:

1. Join the *EI-ISAC*.
2. *Protect your website* with simple and free tools.
3. Implement an *endpoint protection* program through a commercial provider or for free through the EI-ISAC.
4. Implement the *malicious domain blocking and reporting* tool for free through the EI-ISAC.
5. Manage your *removable media*.

4.2 Level 2 and Level 3 Maturities

More mature organizations should take a more sophisticated approach to prioritizing best practice implementation.

4.2.1 The CIS Community Defense Model

To help organizations determine where to invest their next dollar in cybersecurity, CIS developed the *Community Defense Model* (CDM). The CDM was created to help answer that and other questions about the value of the *CIS Controls* based on currently available threat data from industry reports. Ready more about the CIS Controls in the CIS Controls *best practice*.

Using authoritative data sources like the Verizon Data Breach Investigations Report, CIS identified the top attack types that enterprises should defend against.

For CDM 2.0, the top five attack types are:

1. Malware
2. Ransomware
3. Web Application Hacking
4. Insider and Privilege Misuse
5. Targeted Intrusions

Certain techniques are used to execute each of these types of attacks. The CDM uses the MITRE ATT&CK framework to cateogize these techniques and sub-techniques. These are mapped to mitigations, such as the Safeguards contained with the CIS Controls and the actions within this Guide's best practices, that protect against one or more sub-technique.

Using real world data, the CDM determines which Safeguards are the most efficient–the Safeguards that mitigate the most sub-techniques and thus, when implemented, are most likely to stop any given attack.

In the table below, we map the highest efficiency Safeguards from the CIS Controls to the best practices in this Guide to establish the priority best practices. For more details on the efficiency rankings, see Figure 13 of the CDM 2.0.

Table 1: Mapping of the Most Efficient Safeguards to Priority Best Practices

Rank	Safeguard	Safeguard Title	Essential Guide Best Practice
1	4.1	Establish and Maintain a Secure Configuration Process	*Managing Infrastructure*
2	4.7	Manage Default Accounts on Enterprise Assets and Software	*Managing Infrastructure*
3	5.3	Disable Dormant Accounts	*User Management*
4	6.1	Establish an Access Granting Process	*User Management*
5	6.2	Establish an Access Revoking Process	*User Management*
6	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	*Managing Infrastructure*
7	18.3	Remediate Penetration Test Findings	[Coming in 2022Q3 update]
8	18.5	Perform Periodic Internal Penetration Tests	[Coming in 2022Q3 update]
9	6.8	Define and Maintain Role-Based Access Control	*User Management*
10	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	*Managing Infrastructure*
11	3.12	Segment Data Processing and Storage Based on Sensitivity	[Coming in 2022Q3 update]
12	5.2	Use Unique Passwords	*User Management*
13	6.4	Require MFA for Remote Network Access	*Managing Remote Connections*
14	6.5	Require MFA for Administrative Access	*User Management*
15	12.8	Maintain Dedicated Computing Resources for All Administrative Work	*Managing Infrastructure*
16	2.3	Address Unauthorized Software	*Asset Management*
17	2.5	Allowlist Authorized Software	*Asset Management*
18	4.2	Maintain a Secure Configuration Process for Network Infrastructure	*Managing Infrastructure*
19	4.4	Implement and Manage a Firewall on Servers	*Firewalls and Port Restrictions*
20	6.3	Require MFA for Externally-Exposed Applications	*User Management*

The best practices in the right column are listed as priority actions in the *best practice index* and should be implemented first for the Level 2 and Level 3 maturities.

CHAPTER

FIVE

INDEX OF BEST PRACTICES

The following table lists the best practices and indicated if they have actions associated with them for each maturity level ("In Scope" or "Out of Scope") and if they are a priority action ("Priority") for each maturity level.

For more details on maturities in this Guide, see the *maturities descriptions*.

To learn how to determine the maturity at which your organization operates, see the *maturity determination* guide.

For a better understanding of how these priorities were determined and for a better understanding of how to start implementing these best practices, see the maturity to best practice *mapping*.

You can use this table as a checklist to help track your progress.

✓	Best Practice	Maturity Priorities		
		Level 1	Level 2	Level 3
	Addressing Physical Threats	In scope	In scope	In scope
	Asset Management	Priority	Priority	Priority
	Backups	Priority	Priority	Priority
	Building and Managing Staff	Priority	Priority	Priority
	Encrypt Data at Rest	Priority	Priority	Priority
	Endpoint Protection	In scope	In scope	In scope
	Exercising Plans	In scope	In scope	In scope
	Firewalls and Port Restrictions	In scope	Priority	Priority
	Formal Cybersecurity Assessments	In scope	In scope	In scope
	Implementing the CIS Controls	In scope	In scope	In scope
	Incident Response	Priority	Priority	Priority
	Join the EI-ISAC	Priority	Priority	Priority
	Malicious Domain Blocking & Reporting	In scope	In scope	In scope
	Managing Infrastructure	Priority	Priority	Priority
	Managing Mis-, Dis-, and Malinformation	In scope	In scope	In scope
	Managing Remote Connections	In scope	Priority	Priority
	Managing Removable Media	In scope	In scope	In scope
	Managing Vendors	In scope	In scope	In scope
	Managing Wireless Networks	In scope	In scope	In scope
	Network Monitoring and Intrusion Detection	Out of scope	In scope	In scope
	Patching and Vulnerability Management	In scope	In scope	In scope
	Public Facing Network Scanning	In scope	In scope	In scope
	User Management	Priority	Priority	Priority
	Website Security	In scope	In scope	In scope

CHAPTER

SIX

ADDRESSING PHYSICAL THREATS

Sadly, in the last several years, election officials have been subjected to increased threats, harassment, and doxing, causing a significant negative impact on their personal lives as well as interfering with the secure operation of our government processes and election infrastructure.

Officials are used to receiving emails, voicemails, and other contacts that criticize their work. Sometimes these rise to the level of attempts to threaten or intimidate, but attempts to threaten or intimidate are unacceptable, as is doxing–having their personal information published online–which can result in invasions of privacy and increase the risk of physical threats.

There are resources available to help and support you and your team–see below. And if you feel there is any chance of an immediate risk to you or others, do not wait, call 911.

6.1 Goals

1. Know about doxing and how to protect yourself.
2. Know what to do if you encounter an attempt to threaten or intimidate.
3. Know where to get more support.

6.2 Actions

For Addressing Physical Threats, the necessary actions are the same for all maturity levels.

1. Learn about doxing and take action to minimize risk through CISA's Insight on Mitigating the Impacts of Doxing on Critical Infrastructure.
2. If you or anyone in your office receives an attempt to threaten or intimidate:
    - If you feel there is any chance of an **immediate risk to you or others, call 911.**
    - Contact your FBI Elections Crime Coordinator. If you don't know your Election Crimes Coordinator, contact your local FBI field office and ask to speak to the Election Crimes Coordinator.
    - Contact your local CISA Physical Security Advisor (PSA).
3. For additional resources see the Cost Effective Tools section below.

Ensure your entire team is prepared and knows to take these actions if necessary.

6.3 Cost-Effective Tools

- CISA's Insight on Mitigating the Impacts of Doxing on Critical Infrastructure.
- CISA's Security Resources for the Election Infrastructure Subsector.
- U.S. Election Assistance Commission (EAC): Security Resources for Election Officials and Personal Security for Election Officials.
- The Committee for Safe and Secure Elections: https://safeelections.org/.
- Contact elections@cisecurity.org for more information.

6.4 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

6.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

CHAPTER

SEVEN

ASSET MANAGEMENT

Without a clear understanding of what computers and other technology you must protect, you'll have a hard time ensuring everything you own is properly secured.

There are many free tools that can help automate the job of inventorying and managing physical devices, and for many organizations simple tools like spreadsheets are good enough.

7.1 Goals

1. Maintain proper records of all assets (hardware, software, cloud platforms) throughout their lifecycle (Level 1 maturity)
2. Always know the physical location of hardware (Level 1 maturity)
3. Conduct maintenance and protecting assets from loss, theft, and tampering (Level 1 maturity)

7.2 Actions

For Asset Management, the necessary actions vary by maturity as detailed below.

7.2.1 Level 1 Maturity

For those organizations operating at a Level 1 maturity, keep it simple. You need to know what physical assets you have, where they are, how they're used, how they're protected, and how they're maintained. Understanding this information will help you properly defend your network and other IT assets.

1. Create an inventory of all state and county technology owned and operated in support of election activities. This includes hardware assets, software, and cloud service providers such as laptops, software suites (e.g., Adobe), and email providers.
    - If you have a fewer than a couple dozen of assets to track, it's probably easiest to do so with a table or spreadsheet. You can do this on paper, though if you use paper, you should also maintain a digital records that you can backup. You can use the Level 1 maturity *IT Inventory Worksheets* as a template or the CIS Enterprise Asset Inventory Worksheet.
    - Even if your county maintains these records, it's best to do so yourself, as you're ultimately accountable for what happens in your environment.
    - Contractor systems should be included in your inventory.
    - This inventory will contain sensitive security information that should not be shared with untrusted parties.

2. Investigate unknown assets discovered during the inventory process. Remove assets that should not be attached to the network. This includes both hardware and software assets.

7.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Maintaining digital inventory records.
2. Applying asset tags.
3. Implementing software tools to discover physical devices on your networks.
4. Allowlist authorized software to prevent unwanted software installation.

Enterprise tools exist to automate this process and if you are at a higher maturity, you should be implementing one of them.

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, mobile device management (*MDM*) tools can support this process, where appropriate.

This inventory should include 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 the control of your organization. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

7.3 Cost-Effective Tools

- CIS Enterprise Asset Inventory Worksheet: An excel workbook suitable for small operations with a limited number of assets
- Nmap: Famous multipurpose network scanner used by system administrators and hackers across the world to identify which devices are connected to your network
- ZenMap: Easy-to-use graphic user interface for Nmap
- Spiceworks: Free IT inventory and asset management software to identify devices and software on your network

7.4 Mapping to CIS Controls and Safeguards

- 1.1: Establish and Maintain Detailed Enterprise Asset Inventory (Level 1 maturity)
- 1.2: Address Unauthorized Assets (Level 1 maturity)
- 2.3: Address Unauthorized Software (Level 1 maturity)
- 1.3: Utilize an Active Discovery Tool (Level 2 maturity)
- 2.5: Allowlist Authorized Software (Level 2 maturity)
- 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory (Level 3 maturity)

7.5 Mapping to CIS Handbook Best Practices

- 23, 27, 28, 30, 45, 55, 65, 67, 68, 69, 79, 86, 88

CHAPTER

EIGHT

BACKUPS

Backups are necessary due to the constant threat of modification or erasure of data due to accidental deletions, *malware* (including *ransomware*), natural disasters, or other events. Good backup practices are especially important during critical points of operational cycles, like the beginning of early voting.

Backups play a crucial role in expediting the recovery from malicious cyber activity, allowing the restoration of a system to a reliable state that is free of malware and retains the original data. Rebuilding or re-imaging an infected system from a known good backup or fresh operating system installation is a common best practice in incident response. For instance, if an elections network is compromised due to malware, restoring systems from a clean, uncompromised backup will allow the system to be quickly remediated and put back into production without having to wait to identify remove all possible malicious files.

Backup programs should be developed based on six characteristics:

1. **Data Classification:** Knowing what you want to backup will help you determine what and how frequently that data should be backed up. For instance, data vital to election operations, such as voter registration information, would be considered a high priority, and the risk management process may justify the use of nightly full backups. Retention requirements can play a role in classification.
2. **Frequency:** Consider how much data loss would be acceptable in the event of a catastrophic failure. The amount of data that would be acceptable to lose (e.g., 24 hours' worth) should then be used to determine how often data should be backed up.
3. **Encrypted:** Backups should be encrypted. Having the backup encrypted will safeguard it if an unauthorized individual tries to access it.
4. **Offline:** Backups must be stored offline to reduce the risk of malware infecting the copies. Some malware, such as ransomware, will specifically look for backups that are available on the network to hinder the recovery process.
5. **Offsite:** Backups should be stored offsite to ensure recovery is possible in the event of disasters, such as fire or flooding. Offsite backups could be physical copies or cloud-based. The backup location is vital to the recovery process and must be a place where the backups will be secure but quickly accessible.
6. **Tested:** Testing the backup's integrity and the ability to successfully restore a system from the backup is essential to a successful restoration. This ensures that, if needed, the backups will be able to restore what has been corrupted or destroyed. Too often backups are untested and can't actually be restored in times of crisis.

8.1 Goals

1. Create a procedure for backups
2. Implement automated backups
3. Protect backups
4. Test your recovery plan

8.2 Actions

For Backups, the necessary actions vary by maturity as detailed below.

8.2.1 Level 1 Maturity

Creating a data inventory for a Level 1 maturity organization should include at a minimum:

1. Create a data inventory to understand the most important data residing within your network. Include, at a minimum:
    - Voter registration information and databases
    - Ballot definitions
    - Election equipment security processes
    - Geopological boundary data and shapefiles
    - Other critical data
2. Ensure data critical to the operation of your state organization or local jurisdiction is backed up and stored offsite.

There are many automated methods for creating backups. Most solutions are encrypted and can be set to the desired frequency. But many are only either offline or offsite, whereas both are necessary to have a complete backup program. Offline backups help protect from ransomware, while offsite backups help protect from local disasters.

Simple built-in backup tools like Apple's Time Machine and Microsoft's Backup and Restore work well for offline backups if they are not kept connected to a network or machine. If you wish to use tools like this, be sure to have a plan to connect them on a prescribed schedule and then promptly remove, isolate, and securely store them. Unless you move them to other locations, they are not good solutions for offsite backups.

Either implement a tool that provides both offline and offsite backup capabilities or implement multiple tools. Some are described below within Cost-Effective Tools.

8.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Ensure that solutions conform to your data management plan.
2. Test backups at least once a quarter and whenever processes or technologies are changed. The goal is ensuring rapidly restoration of operations, if ever needed.

8.3 Cost-Effective Tools

- Apple Time Machine: Time Machine is the backup mechanism of macOS, the desktop operating system developed by Apple. The software is designed to work with both local storage devices and network-attached disks and is most commonly used with external disk drives connected using either USB or Thunderbolt.
- Amanda Network Backup: AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup solution that allows the IT administrator to set up a single master backup server to back up multiple hosts over network to tape drives/changers or disks or optical media. Amanda uses native utilities and formats (e.g. dump and/or GNU tar) and can back up a large number of servers and workstations running multiple versions of Linux or Unix. Amanda uses a native Windows client to back up Microsoft Windows desktops and servers.
- Bacula: Bacula is a set of Open Source computer programs that permit you (or the system administrator) to manage backup, recovery, and verification of computer data across a network of computers of different kinds.
- Microsoft Backup & Restore: In Windows 11, you can restore files from a backup created with Backup and Restore or File History.
- DHS, CISA, and MS-ISAC Joint Ransomware Guide: A guide written by US federal agencies to assist with ransomware.

8.4 Mapping to CIS Controls and Safeguards

- 11.1: Establish and maintain a data recovery process (Level 1 maturity)
- 11.2: Perform automated backups of in-scope enterprise assets (Level 1 maturity)
- 11.3: Protect recovery data (Level 1 maturity)
- 11.4: Establish and maintain an isolated instance of recovery data (Level 1 maturity)
- 11.5: Test backup recovery (Level 2 maturity)

8.5 Mapping to CIS Handbook Best Practices

- 21, 60

CHAPTER

NINE

BUILDING AND MANAGING STAFF

Cybersecurity is more than technology and processes. People are at the heart of any cybersecurity program. This means hiring people you can trust with the sensitive tasks they have to complete and giving them the tools they need to be successful.

Background checks, including criminal and financial checks, are essential for a healthy hiring process. In addition, carefully manage staff access, both physical and electronic, and provide them the training they need so they can make good cybersecurity decisions.

9.1 Goals

1. Conduct background checks for new hires (Level 1 maturity)
2. Use available cybersecurity training to improve your cybersecurity posture (Level 1 maturity)

9.2 Actions

For Building and Managing Staff, the necessary actions are the same for all maturity levels.

1. Conduct at least a national agency check for any hires. Your state or county may have other background check options for you.
2. Provide security awareness training for all staff.
3. Track training either through a human resources portal or manually through a worksheet. You can use the Level 1 maturity *Cyber Education worksheet* as a template.
4. Implement actions for proper logical access in *User Management*
5. Implement actions for proper system configuration in *Managing Infrastructure*

9.3 Learn More

- Learn how to protect yourself, your family and your devices with tips and resources from the National Cybersecurity Alliance (https://staysafeonline.org/stay-safe-online).

9.4 Mapping to CIS Controls and Safeguards

- 14.1: Establish and Maintain a Security Awareness Program (Level 1 maturity)
- 14.2: Train Workforce Members to Recognize Social Engineering Attacks (Level 1 maturity)
- 14.3: Train Workforce Members on Authentication Best Practices (Level 1 maturity)
- 14.4: Train Workforce on Data Handling Best Practices (Level 1 maturity)
- 14.5: Train Workforce Members on Causes of Unintentional Data Exposure (Level 1 maturity)
- 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents (Level 1 maturity)
- 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates (Level 1 maturity)
- 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks (Level 1 maturity)
- 14.9: Conduct Role-Specific Security Awareness and Skills Training (Level 2 maturity)

9.5 Mapping to CIS Handbook Best Practices

- 13, 16, 54, 57, 58, 59, 82, 87

CHAPTER

TEN

ENCRYPT DATA AT REST

Any data that is not being actively transferred can be referred to "data at rest." This includes data residing on hard drives, USB sticks, and with third-party cloud service providers. Encryption allows for data at rest to be properly secured. For instance, encrypting personally identifiable information (PII) with strong encryption algorithms protects the data from accidental disclosure in the case of a data breach.

Elections offices may maintain a number of systems that must use encryption and are responsible for identifying data that should be encrypted.

In modern laptops, desktops, and server environments, encryption capabilities of some form are often built into the software and hardware stack. These capabilities may be enabled by default or will need to be properly configured. Third-party encryption utilities may also be needed to encrypt specific data, such as within an application, database, or a USB device.

10.1 Goals

1. Enable encryption for laptops, desktops, servers, and mobile devices, known as full-disk encryption (Level 1 maturity)
2. Encrypt backups (Level 1 maturity)
3. Encrypt removable devices, where practical, such as with USB devices (Level 2 maturity)

10.2 Actions

For Encrypt Data at Rest, the necessary actions vary by maturity as detailed below.

10.2.1 Level 1 Maturity

1. Enable encryption, often called full-disk encyrption, on all devices that have encryption technologies built into the device.
    - You can use the Level 1 maturity *Asset Protection worksheet* as a template to track your work.
    - The *cost effective tools* section below may help, depending on the types of systems you have in your environment.
2. Encrypt backups. Use the *backups* best practice as a guide.

10.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Work with those who provide IT infrastructure, whether vendors or your own IT staff, to implement encryption for all sensitive data.
2. Implement encryption when data is at rest (e.g., stored in a database or on a device) and in transit (e.g., sending through email) and ensure all encryption meets your election office's adherence to encryption standards.

The National Institute of Standards and Technology (*NIST*) Special Publication 800-175B provides the U.S. federal requirements for encryption standards to secure data at different sensitivity and classification levels.

NIST Special Publication 800-122 provides the U.S. federal requirements for protecting the confidentiality of personal information.

10.3 Cost-Effective Tools

- Bitlocker: Built-in encryption for supported Microsoft® Windows devices.
- FileVault: Built-in encryption for MacOS devices.
- Veracrypt: Open-source, free full disk encryption utility.
- EaseUS: This free program can encrypt system images.

10.4 Mapping to CIS Controls and Safeguards

- 3.6: Encrypt Data on End-User Devices
- 3.9: Encrypt Data on Removable Media
- 3.11: Encrypt Sensitive Data at Rest
- 11.3: Protect Recovery Data

10.5 Mapping to CIS Handbook Best Practices

- 4, 12, 84

CHAPTER

ELEVEN

ENDPOINT PROTECTION

Endpoint protection is security software that is deployed on workstations and servers, which are commonly referred to as "endpoints." A common name for this is *Endpoint Detection and Response*, or *EDR*. EDR collects technical data from these endpoints and transmits it back to the vendor or a local server. The data is then analyzed for suspicious patterns and threats.

If a threat is identified, it is blocked, and an alert is generated. Administrators can typically view alerts through a vendor control panel or a connection to their own security platform. Also, many *EDR* solutions include a traditional antivirus functionality and the ability for responders to remotely access compromised systems for remediation.

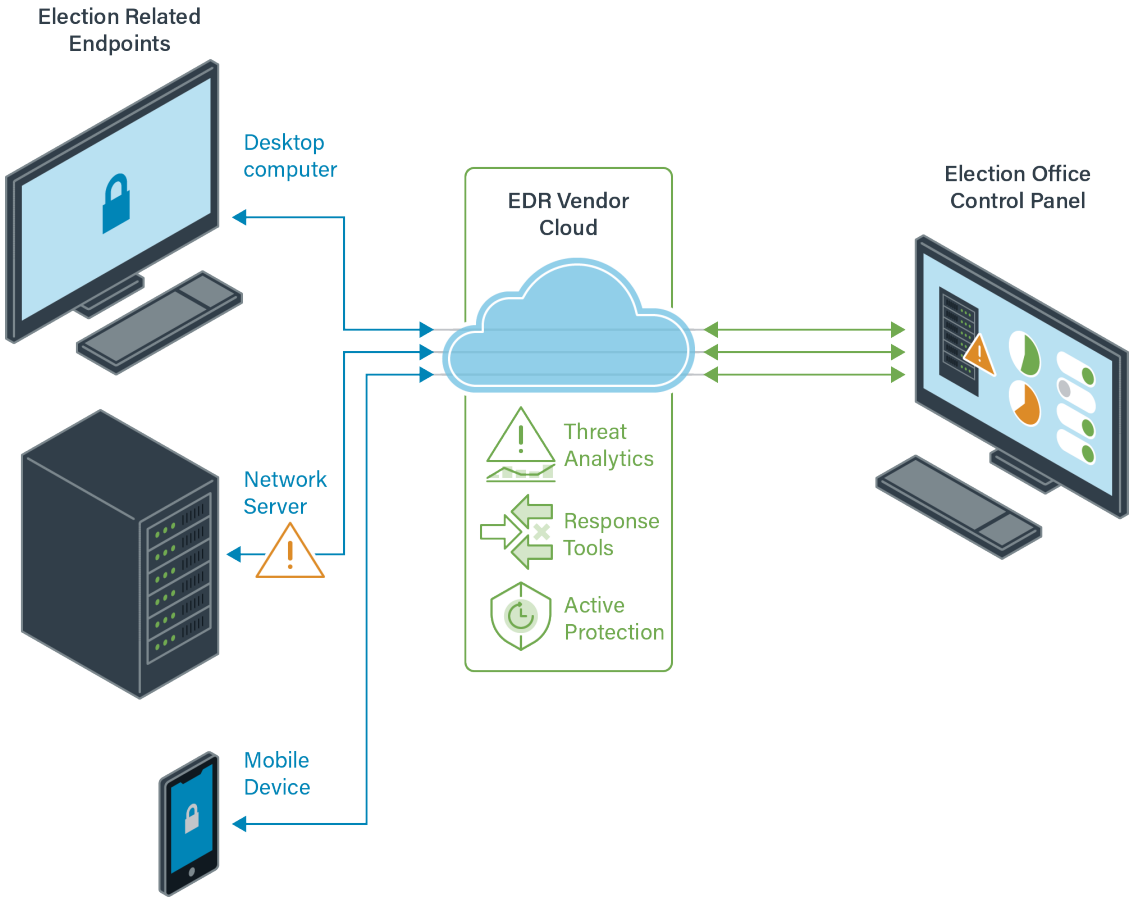


Fig. 1: *EDR* with a Cloud-based Vendor Solution

Election offices can use *EDR* to:

- Detect and stop active attacks on election infrastructure,
- Protect against malware,
- Quarantine suspicious files,
- Isolate compromised systems,
- Remediate malware infections,
- Enable analysis to find and mitigate threats, and
- Disable and restrict the ability of suspicious users on your network to cause harm.

Election officies should put EDR on internet-connected and critical endpoints, including workstations, mobile devices, webservers, and other important networked systems. EDR should not be deployed on voting systems.

11.1 Goals

1. Get EDR services through the EI-ISAC or commercial vendors (Level 1 maturity)

11.2 Actions

For Endpoint Protection, the necessary actions vary by maturity as detailed below.

11.2.1 Level 1 Maturity

1. Deploy EDR on systems throughout your network. EDR should not be deployed on voting systems.
    - All your systems and endpoints that touch administrative election processes are covered at no cost to you by the federally-funded EDR program. Additionally, your jurisdiction's non-election endpoints can also sign up for the same services at a discounted cost. Contact elections@cisecurity.org for more information.
    - For commercial solutions, you may also review CIS's Guide for Ensuring Security in Election Technology Procurements for best practices in crafting proposals and other necessary documents.
2. Take advantage of vendor-offered user training for usage of EDR tools, including when you sign up for the EI-ISAC EDR program.
3. Implement best practices for EDR:
    - Delegate personnel to monitor and act on detections.
    - Export information regularly from the control panel to local hardware backups, so you always have access to data needed for audits and investigations.
    - Consider available staffing resources to support any new security infrastructure and the associated responsibilities. Many EDR providers offer solutions supported by a 24×7 team to manage and respond to identified incidents.
    - Refer to the EI-ISAC Cyber Incident Checklist to manage security events.

11.2.2 Level 2 and Level 3 Maturities

For the Level 2 and Level 3 maturities, all of the guidance for the Level 1 maturity applies, but the specifics of your network configuration and the number of endpoints you serve may affect whether you can implement EDR through the EI-ISAC. Contact elections@cisecurity.org for more information.

11.3 Cost-Effective Tools

- EI-ISAC EDR program: EDR services at no charge to state and local election offices.(Contact elections@cisecurity.org)

11.4 Learn More

- EI-ISAC EDR program brochure

11.5 Mapping to CIS Controls and Safeguards

- 10.1: Deploy and Maintain Anti-Malware Software
- 10.6: Centrally Manage Anti-Malware Software

11.6 Mapping to CIS Handbook Best Practices

- 32, 40

CHAPTER

TWELVE

EXERCISING PLANS

Exercising a plan before it is needed is almost as important as having the plan in the first place. Virtually any type of plan can be exercised, including normal operations and in the face of network disruptions, physical threats, disinformation, power outages, and many other types of incidents.

Generally, you can either take part in exercises offered by others – such as a state election office or CISA – or run your own exercises internally. Both are important. Internal exercises will test your own plans and your ability to execute on them. External exercises will further test those plans and introduce ideas you may not have considered.

12.1 Goals

1. Learn the types of exercises that make sense for your organization (Level 1 maturity)
2. Participate in exercises or create your own (Level 1 maturity)

12.2 Actions

For Exercising Plans, the necessary actions vary by maturity as detailed below.

12.2.1 Level 1 Maturity

1. Participate in CISA's annual Tabletop the Vote exercise through your state leadership.
2. Your state may have other exercises. Contact your state election director and consider participating in these as well.
3. Have plans for other incidents and exercise them at least annually. While facilitated exercises are preferred, an internal tabletop-style walkthrough is better than nothing.

12.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Consider participating in other exercises or creating your own with the CISA critical infrastructure exercise guides.
2. Have a regular schedule for exercises. Stick to it.

12.3 Mapping to CIS Controls and Safeguards

- 17.1: Designate Personnel to Manage Incident Handling
- 17.2: Establish and Maintain Contact Information for Reporting Security Incidents
- 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
- 17.4: Establish and Maintain an Incident Response Process
- 17.5: Assign Key Roles and Responsibilities
- 17.6: Define Mechanisms for Communicating During Incident Response
- 17.7: Conduct Routine Incident Response Exercises
- 17.8: Conduct Post-Incident Reviews
- 17.9: Establish and Maintain Security Incident Thresholds

12.4 Mapping to CIS Handbook Best Practices

- 33, 72

CHAPTER

THIRTEEN

FIREWALLS AND PORT RESTRICTIONS

Firewalls are an important part of cyber defense. You can set policies to manage firewalls to prevent unwanted behavior and reduce the risk of successful attack. On the other hand, a poorly protected firewall or bad configuration decisions can give threat actors an opportunity to gain access to private assets and resources.

Attackers search for vulnerable default settings and gaps or inconsistencies in firewall rule sets, routers, and switches, then 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.

All firewalls, no matter how simple or small of a network, need to have their configurations managed. To properly manage network firewalls, you need to establish rules and policies, track changes, and monitor compliance logs. You should also implement and manage firewalls on end user devices.

13.1 Goals

1. Enable network scanning to look for port vulnerabilities (Level 1 maturity)
2. Enable firewall management on networks (Level 1 maturity)
3. Enable firewall management on end-user devices (Level 1 maturity)

13.2 Actions

For Firewalls and Port Restrictions, the necessary actions vary by maturity as detailed below.

13.2.1 Level 1 Maturity

Manage firewalls on all servers and end-user devices.

1. Use free tools and services to conduct scans of your publicly-facing assets. This should include your website and any online portals you are responsible for that are used for elections purposes. Sign up for free vulnerability scanning by contacting CISA at vulnerability_info@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services."
2. Change default passwords for all applications, operating systems, routers, firewalls, wireless access points, printers, scanners, and other devices when adding them to the network.
3. Block all access by default, then allow-list traffic you want on the network.
4. Update firewall software automatically or on a set schedule. Stick to that schedule.
5. Limit administrative access to the firewalls to as few individuals as possible.

6. Review firewall rules on a set schedule. Stick to that schedule.

13.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Implement a CIS Benchmark for firewall management.

13.3 Cost-Effective Tools

- Free vulnerability scanning from CISA (contact vulnerability_info@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services")
- CIS Benchmark for firewall management

13.4 Mapping to CIS Controls and Safeguards

- 4.4: Implement and Manage a Firewall on Servers (Level 1 maturity)
- 4.5: Implement and Manage a Firewall on End-User Devices (Level 1 maturity)
- 13.9: Deploy Port-Level Access Control (Level 3 maturity)
- 13.10: Perform Application Layer Filtering (Level 3 maturity)

13.5 Mapping to CIS Handbook Best Practices

- 41, 42

CHAPTER

FOURTEEN

FORMAL CYBERSECURITY ASSESSMENTS

A security assessment is a thorough, proactive study of an organization's systems that helps identify security challenges and implement solutions. Assessments help identify and prevent security issues, meet national standards, and gain voter trust. They can also justify a budget and guide procurements of security resources, tools, and services.

Formal cybersecurity assessments are a fundamental aspect of managing cybersecurity risk. Assessments can take many forms, but good ones are based on a highly-accepted risk framework, like ISO 27000 series, the NIST Cybersecurity Framework, and the CIS Controls.

Most importantly, you need to be prepared to do something about the results of your assessments. Most will provide some prioritization of results. Once you have these results, develop a plan of action and milestones to get issues addressed.

Risk assessments are a common form of assessment that can be sorted into two categories:

1. Self-assessments: In-house risk assessments are generally faster and less expensive while still providing useful insight into your cybersecurity posture.
2. Independent assessments: Because they are conducted by outside assessment specialists, independent assessments usually cost more and take longer, but they are more objective and thorough. Where time and resources permit, they are preferable even when an organization has deep cybersecurity experience.

14.1 Goals

1. Understand and determine the type and extent of cybersecurity assessment your organization should undergo (Level 1 maturity)
2. Use the results to improve your cybersecurity posture (Level 1 maturity)
3. Implement a risk assessment program (Level 2 maturity)

14.2 Actions

For Formal Cybersecurity Assessments, the necessary actions vary by maturity as detailed below.

14.2.1 Level 1 Maturity

1. Choose a type of assessment.
2. Perform a security assessment.
3. Receive results of the assessment.
4. Do something about the results.

Keep it simple. If you haven't implemented the critical actions for the Level 1 maturity yet, start with those. If you have, consider stepping up to vulnerability scanning or a risk and vulnerability assessment. Review the CISA's CyHy site or contact CISA at vulnerability_info@cisa.dhs.gov for more information.

Whatever you choose to do, figure out how often you should do it, stick to it, and add to it when resources permit.

14.2.2 Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Consider a more robust assessment program. While conducting large assessments can provide significant information about your systems and put you in a great position to harden them, they can be expensive and resource-intensive.
2. Focus on automated or structured tools and services for understanding your systems. There are many options available to you.
    - Review the options CISA offers through its resource hub with your technical staff and decide which services make sense for you and how often you should use them.
3. Consider implementing the CIS Controls and CIS Benchmarks.
    - Tools available to election offices include CIS-CAT, which can automate much of the process of implementing appropriate safeguards.

14.2.3 Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Implementing sophisticated controls and undergoing both internal and independent assessments. All of the tools mentioned above are still in play for you, but you should be implementing them as part of a well-crafted overall plan. Build this into your program documentation, track progress, and seek new ways to conduct regular, automated, or continuous monitoring of your risk framework.

14.3 Cost-Effective Tools

- CISA Cyber Hygiene Services: CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Types of scans and assessments include vulnerability scanning, web application scanning, phishing campaign assessments, and remote penetration testing. (https://www.cisa.gov/cyber-hygiene-services)
- CIS Controls: see the *CIS Controls* best practice
- CIS Benchmarks: Secure configurations for more than a hundred of the most common software applications. (https://www.cisecurity.org/cis-benchmarks/)
- CIS-CAT: a tool freely available to *EI-ISAC members* to support implementation of the CIS Controls

14.4 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls, though assessments can be conducted against the CIS Controls using the tools listed above.

14.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

CHAPTER

FIFTEEN

IMPLEMENTING THE CIS CONTROLS

The CIS Critical Security Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a consensus-based community of cybersecurity experts and are globally accepted security best practices.

Within each of the 18 CIS Controls is a set of safeguards focused on a specific security function. There are a total of 153 safeguards. Experience has shown that organizations of every size and complexity need help to get started with the CIS Controls, and to focus their attention and resources.

The CIS Implementation Groups (*IGs*) were created to address this need. These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

The CIS Controls are organized into IGs, each with its own unique list of Safeguards. The IGs are defined according to three attributes:

1. Data sensitivity and criticality of services offered by the organization
2. Expected level of technical expertise exhibited by staff or on contract
3. Resources and expertise available and dedicated toward cybersecurity activities

This results in three IGs, and the maturities in this Guide are loosely based on those IG classifications:

- **IG1: Basic.** Contains controls that help an organization assess its current security and take simple steps to improve it. Roughly equivalent to the Level 1 maturity.
- **IG2: Foundational.** Contains more advanced guidance to improve an organization's security. Roughly equivalent to the Level 2 maturity.
- **IG3: Organizational.** Contains controls that make changes to an organization's policies to improve and maintain their cybersecurity. Roughly equivalent to the Level 3 maturity.

15.1 Goals

1. Implement the appropriate IGs for your organization (Level 1 maturity)

15.2 Actions

For Implementing the CIS Controls, the necessary actions vary by maturity as detailed below.

15.2.1 Level 1 Maturity

1. Implement the IG1 controls.
    - The easiest way to do this is through the Level 1 *Priorities*. This will help you complete all of the actions for the Level 1 maturity, including IG1.
    - You can also use the CIS Controls Navigator to get to export a convenient list of the IG1 controls.

15.2.2 Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Implement the IG2 controls. Use the CIS Controls Navigator to get this done.

15.2.3 Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Implement all of the CIS Controls that are applicable for your environment. Use the CIS Controls Navigator to get this done.

15.3 Cost-Effective Tools

- CIS Controls Navigator: A simple tool to allow export of customized sets of safeguards from the CIS Controls.
- CIS Controls version 8: A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

15.4 Mapping to CIS Controls and Safeguards

- All!

15.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

CHAPTER

SIXTEEN

INCIDENT RESPONSE PLANNING

From power failures to flooding to malicous cyber attacks, incidents occur. While the type of incident and sophistication of the threat actors plays a major role in the outcomes, often the difference between minor and severe consequences have more to do with how you prepare for and respond to the incident.

To get back up and running quickly after an incident, you have to plan well. This means developing written plans – often called incident response plans, disaster recovery plans, or business continuity plans. It also means testing those plans through exercises.

16.1 Goals

1. Develop and maintain an incident response plan (Level 1 maturity)
2. Exercise your plans (Level 1 maturity)
3. Conduct after-action reports following and incident (Level 2 maturity)

16.2 Actions

For Incident Response Planning, the necessary actions vary by maturity as detailed below.

16.2.1 Level 1 Maturity

1. Create and maintain an incident response plan.
    - Include relevant stakeholders from the various business units that may be impacted.
    - Identify and prioritize critical systems.
    - There are many resources available to help you out, including:
        - The Election Assistance Commission's tips for disaster planning.
        - CISA's Incident Response Support for Election Partners.
        - The Belfer Center's Election Playbook.
2. *Exercise your plan* regularly. At least once a year; before each election is better.
3. When an incident does occur, execute your plan.
    - The EI-ISAC is here to help during an incident. Contact soc@cisecurity.org.
4. Regularly review the your plan to ensure contacts are up to date and procedures are still effective and relevant

16.2.2 Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. When an incident does occur, conduct an after action reviews to identify what went right, what went wrong, and make improvements to your plan.

16.3 Mapping to CIS Controls and Safeguards

- 11.1: Establish and Maintain a Data Recovery Process (Level 1 maturity)
- 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents (Level 1 maturity)
- 17.1: Designate Personnel to Manage Incident Handling (Level 1 maturity)
- 17.2: Establish and Maintain Contact Information for Reporting Security Incidents (Level 1 maturity)
- 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents (Level 1 maturity)
- 17.4: Establish and Maintain an Incident Response Process (Level 2 maturity)
- 17.5: Assign Key Roles and Responsibilities (Level 2 maturity)
- 17.6: Define Mechanisms for Communicating During Incident Response (Level 2 maturity)
- 17.7: Conduct Routine Incident Response Exercises (Level 2 maturity)
- 17.8: Conduct Post-Incident Reviews (Level 2 maturity)
- 17.9: Establish and Maintain Security Incident Thresholds (Level 3 maturity)

16.4 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

CHAPTER

SEVENTEEN

JOIN THE EI-ISAC

CIS and the EI-ISAC are available to provide a wide range of resources to support the cybersecurity needs of the election community. The EI-ISAC and Multi-State ISAC (*MS-ISAC*) are supported by CISA, and all three provide tools, resources, and support to election officials.

Membership in the EI-ISAC is open to all state, local, tribal, and territorial government organizations that support election administration of the United States of America and associations thereof. It's a free and voluntary membership for eligible organizations.

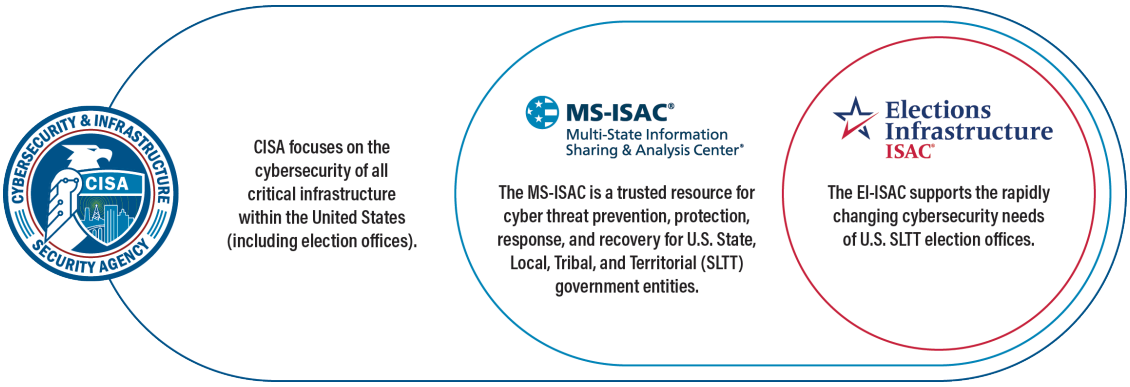


Fig. 1: Relationship between CISA, the MS-ISAC, and the EI-ISAC

The EI-ISAC provides access to valuable services to fulfill many of the best practices described elsewhere in this Guide. Some of them include:

- *Malicious Domain Blocking & Reporting*
- *Endpoint Detection and Response*
- Implementing and managing risk to the *CIS Controls*
- *Network monitoring* via the Albert sensor
- Support for *addressing misinformation* on social media networks
- 24×7×365 Security Operations Center (SOC)
- Training and awareness materials
- Cyber incident resources
- Cyber defense tools
- Webinars and threat briefings
- Cyber threat information

- CIS SecureSuite® Membership
- Discounts on training
- Homeland Security Information Network (HSIN) portal access

17.1 Goals

1. Understand what the EI-ISAC has to offer (Level 1 maturity)
2. Join the EI-ISAC (Level 1 maturity)

17.2 Actions

For Join the EI-ISAC, the necessary actions are the same for all maturity levels.

1. Join the EI-ISAC. Simply sign up here.
    - Contact the EI-ISAC at elections@cisecurity.org with any questions about membership.

17.3 Cost-Effective Tools

- The EI-ISAC has many tools available once you become a member. https://learn.cisecurity.org/ei-isac-registration

17.4 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

17.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

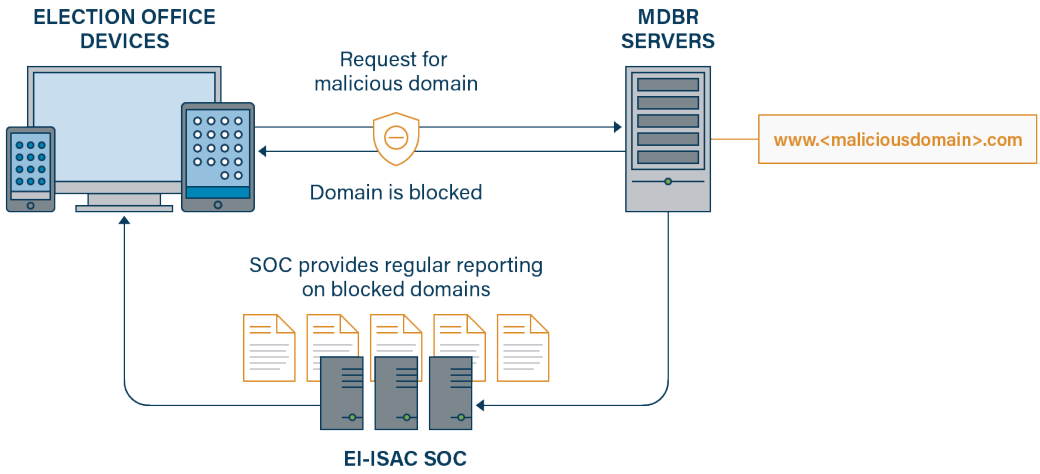
CHAPTER

EIGHTEEN

MALICIOUS DOMAIN BLOCKING AND REPORTING

Malicious Domain Blocking and Reporting, or *MDBR*, technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

Once an organization points its domain name system (*DNS*) requests to the MDBR DNS server IP addresses, every DNS lookup will be compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, are blocked and logged.



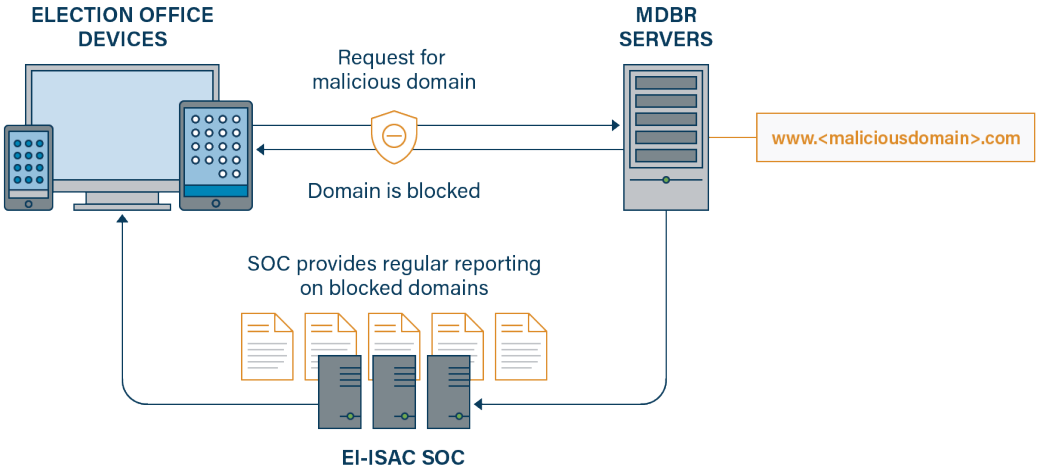


Fig. 1: *MDBR* in an election office environment

18.1 Goals

1. Deploy MDBR for all internet-facing IT assets (Level 1 maturity)

18.2 Actions

For Malicious Domain Blocking and Reporting, the necessary actions are the same for all maturity levels.

1. If you're an EI-ISAC member, you can sign up for no-cost MDBR by registering at https://mdbr.cisecurity.org. You will be asked to provide the following information:
    - Your contact information
    - Technical contact(s) for MDBR setup, troubleshooting, and general technical support
    - Reporting contact(s) for receiving reports on your MDBR service
    - Public IP addresses or CIDR netblocks from which your organization's DNS queries are sent
2. If you aren't an MS-ISAC or EI-ISAC member, *join today* – then complete action #1

The EI-ISAC provides members with a free MDBR service. Members sign up and configure their DNS server, and the EI-ISAC will then provide reporting that includes log information for all blocked requests and assist in remediation if needed.

The service is easy to implement and requires virtually no maintenance as EI-ISAC and its provider fully maintain the systems required to provide the service.

The EI-ISAC hosts all reporting data, including both successful and blocked DNS requests. It will then perform detailed analysis and reporting for the organization and the election community writ large. The EI-ISAC will provide regular reporting and intelligence services for SLTT members.

18.3 Cost-Effective Tools

- EI-ISAC MDBR service: A no-cost, lightweight MDBR solution for EI-ISAC members [https://mdbr.cisecurity.org]

18.4 Mapping to CIS Controls and Safeguards

- 9.2: Use DNS Filtering Services
- 9.3: Maintain and Enforce Network-Based URL Filters

18.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

CHAPTER

NINETEEN

MANAGING INFRASTRUCTURE

Infrastructure management involves adjusting configuration settings for systems to reduce the risk of cyber attacks. Most workstations (e.g., desktop, laptops, tablets) should have capabilities limited to the job function they serve. Often, this is tied to the type of employee to which the workstation is issued, such as an admin or a poll worker. Sometimes, it's about the use the workstation plays in the office. A similar rule applies to servers and other shared infrastructure.

In general, having a few configurations you use repeatedly is better than creating custom configurations for each system you allow in your environment. You should create these configurations or get them from a trusted source and carefully track any changes to them.

Implementing these configurations can be done manually or with automated tools.

19.1 Goals

1. Properly configure workstation permissions (Level 1 maturity)
2. Leverage CIS Benchmarks for workstation and infrastructure configuration (Level 2 maturity)

19.2 Actions

For Managing Infrastructure, the necessary actions vary by maturity as detailed below.

19.2.1 Level 1 Maturity

1. Limit administrative access to machines that perform administrative functions.
2. If a machine has a short period of inactivity, force a lock screen or log out.
3. Employ the restrictions from the *User Management* best practice.
4. Work with IT staff or vendors to establish a process for configuring network infrastructure to ensure it is secure, consistent, and tracked.

19.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Leverage the CIS Benchmark on workstation management for your operating systems. This will allow for maintenance of a secure configuration process for network infrastructure.
    - Choose stricter security levels for systems with sensitive functions.
    - Consider CIS Benchmarks for servers, desktops, laptops, mobile devices, and software on systems.
    - Use the *EMS* Gateway Benchmark for machines that, through removable media, exchange data with the EMS.
    - Uninstall or disable unnecessary services on enterprise assets and software

19.3 Cost-Effective Tools

- Applocker: Free Microsoft® Windows tool to identify and restrict the software that is allowed to run.
- Netwrix: Variety of free tools to identify information about administrative access on your systems.
- OpenAudIT: Inventory applications and software on workstation servers and network devices.
- CIS Benchmarks.
- EMS Gateway Benchmark.

19.4 Mapping to CIS Controls and Safeguards

- 4.3: Configure Automatic Session Locking on Enterprise Assets (Level 1 maturity)
- 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts (Level 1 maturity)
- 4.2: Maintain a Secure Configuration Process for Network Infrastructure (Level 1 maturity)
- 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work (Level 1 maturity)
- 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software (Level 2 maturity)

19.5 Mapping to CIS Handbook Best Practices

- 23, 27, 65, 68, 88

CHAPTER

TWENTY

MANAGING MIS-, DIS-, AND MALINFORMATION

Mis-, dis-, and mal-information have become a pervasive threat to the election environment. Each has a specific definition. Together, we call them MDM.

- *Misinformation* is false but not created or shared with the intention of causing harm.
- *Disinformation* is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- *Malinformation* is based on fact, but used out of context to mislead, harm, or manipulate.

MDM campaigns are engineered for influence, typically seeking to exploit the psychology of victims' emotions, identities, political affinities, and existing societal rifts.

Both independent threat actors and large nation-state operations are capable of manufacturing MDM. Threat actors may have hundreds of human threat actors on payroll or choose to conduct operations via automated bots. When users encounter inaccurate information or intentional disinformation they may be unable to differentiate it from genuine information, sharing it and unwittingly influencing an even wider audience.

Influencing the political environment through social discourse is a tactic observed in well-funded and complex information attacks, but actors may have competitive, financial, or other motivations as well. Disinformation attacks can function by creating continued influence in a system or sector. Attackers may try to popularize perspectives and viewpoints in target demographics that lead to certain policy or political outcomes. Appearing as authentic citizens or a real customer base on social media, individual disinformation accounts can appeal to users and align with their existing beliefs. Organizations and individuals alike then experience the pressure to act on what is perceived as recurring legitimate messaging but, in reality, is deception.

Often, inaccurate statements about elections are unintentional and just the result of misinformed individuals. As election officials, it's not always important to understand the source or intent of the inaccurate information, but to simply address it with accurate messaging and other remediative action. That is the focus of this best practice.

20.1 Goals

1. Recognize MDM and its potential impact on election administration (Level 1 maturity)
2. Take action when you encounter misinformation (Level 1 maturity)

20.2 Actions

For Managing Mis-, Dis-, and Malinformation, the necessary actions vary by maturity as detailed below.

20.2.1 Level 1 Maturity

At Level 1 maturity, simple steps can help you manage misinformation and address it when it occurs.

Preparing for Mis-, Dis-, and Malinformation

1. Set up *multi-factor authentication* to protect social media accounts from compromise.
2. Use public forums to actively counter misinformation.
3. Regularly publish official messaging about the state of your election infrastructure.
4. Work with local media to promote official sources of information.

Remediating Misinformation

1. Track important information by, for instance, following your county name and the names of your election official and other public figures.
2. Respond to inaccurate information with accurate information as quickly as possible. This rapid response is even more important as an election nears.
3. Election officials can report identified misinformation to misinformation@cisecurity.org.
    - Report anything on social media that's about your jurisdiction, pertains to the administration or security of an election in the United States, and is inaccurate or misleading.
    - Opinions are not misinformation. Only report inaccurate information about election administration itself.
    - Examples include, but aren't limited to, dates of the election, mail ballot rules, ballot information, polling place hours and status, election night reporting procedures, post-election procedures, and voting technology.
    - Include the following information:
        - A screenshot of the social media post and, if possible, the URL.
        - Your name, role, jurisdiction, and work email address.
        - A description of why this is false – not just "this is wrong" but information about why think it's wrong. This doesn't have to be more than a couple sentences, but more detail is better. Citing a law is even better.
        - If appropriate, the EI-ISAC will work to have the inaccurate information removed or labeled.

20.2.2 Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. The Cybersecurity and Infrastructure Security Agency (CISA) offers resources to spot and manage responses to MDM:
    - Recognize the risk of foreign actor operations.
    - Question the source of content and question intent.
    - Investigate the issue for other reliable sources before sharing.
    - Think before you share; disinformation is designed to evoke an emotional response.
    - Talk with your circle about the risks of spreading disinformation.
2. Review the Harvard Kennedy School's Belfer Center publication, "The Election Influence Operations Playbook" for a deeper understanding of these issues and response guidance.
3. Establish a mechanism for the public to report disinformation and misinformation to your office, such as an email or phone number.

20.2.3 Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Consider having a focused workstream to identify and remediate MDM. This can include things like:
    - Tracking hashtags, keywords, and other trends on various social media platforms.
    - Following activity related to your election across a number of platforms, including smaller, niche apps.
    - Contracting with a third party to provide these services for you.
    - If a state, providing services for your locals.

20.3 Cost-Effective Tools

- Election Tools Checklist for combating election misinformation: A framework to help election departments respond to influence operations.
- CISA Rumor Control Page: This page offers the public accurate and authoritative sources of information that will help address common MDM narratives. It is provided by a trusted voice to either preempt or respond to developing narratives.

20.4 Mapping to CIS Controls and Safeguards

There are no relevant CIS Controls.

20.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

CHAPTER

TWENTYONE

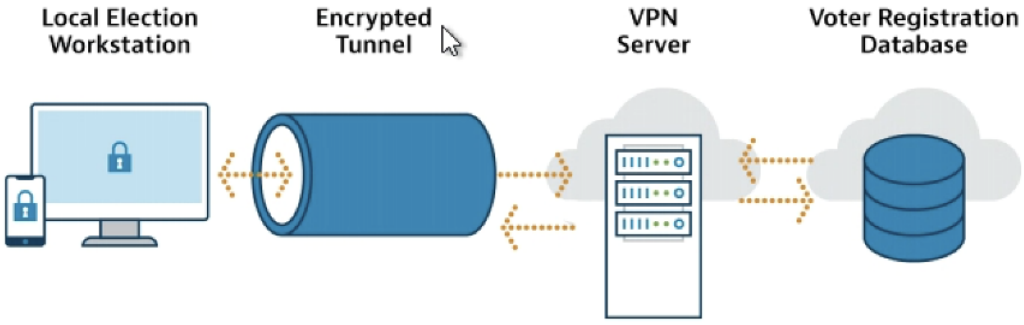
MANAGING REMOTE CONNECTIONS

Remote or traveling employees often require access to enterprise data while physically outside of the workplace. This can be accomplished via a *Virtual Private Network* (VPN). Other common uses include securely connecting on public Wi-Fi, user anonymity, and circumventing government censorship.

VPNs encrypt and transmit data, allowing a user to securely connect to the internet or access a remote network on an untrusted connection. This ensures that all transmitted data remains confidential. Organizations need to authenticate the device or user attempting to establish a *VPN* connection before allowing them access. VPNs can also be used to establish secure connections between two organizations on separate networks.

Many cybersecurity firms offer ready-made hardware and software solutions to deploy a VPN. Well-resourced organizations can also develop their own solutions, such as setting up a VPN router to manage secure connections.

Employees can connect to VPNs via laptops, desktops, or even mobile devices such as smartphones and tablets. When an employee connects to a VPN, it will appear as if they are connecting to the internet from the organization's network, instead of their remote location. Below is a diagram showing how VPNs may be used in an election system.



Election offices can use a VPN to:

- Protect employee data if a remote or offsite employee must connect to an office network, or transmit sensitive data (e.g., employee or election data).
- Securely connect local election officials' workstations to a state voter registration database.
- Securely transmit information to an external partner, such as an election vendor or non-profit organization.

21.1 Goals

1. Understand VPN technology and its role in election environments (Level 1 maturity)
2. Properly implement a VPN service with your environment (Level 1 maturity)

21.2 Actions

For Managing Remote Connections, the necessary actions vary by maturity as detailed below.

21.2.1 Level 1 Maturity

At the Level 1 maturity, organizations should use a VPN for all remote connections. To do so:

1. Recognize situations where a VPN would be useful and appropriate.
2. Implement multi-factor authentication on all VPN connections.
3. Review CIS's Telework and Small Office Network Security Guide for tips on securing a remote work environment.
4. If a trusted third party, like a vendor, provides the VPN used to connect to your network, confirm they are following the same security principles as your organization.

21.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Update the hardware and software used by VPNs and implement a patch management program to prevent malicious actors from exploiting known vulnerabilities. There have been reports of cyber threat actors targeting VPNs by exploiting known vulnerabilities in hardware/software systems.
    - For example, see examples of Common Vulnerabilities and Exposures (*CVE*) here and here, that led to this joint advisory.
2. Review CISA's Enterprise VPN Security Alert
3. Review NIST's Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

21.3 Cost-Effective Tools

- CIS Telework and Small Office Network Security Guide: This Guide is meant to assist individuals and organizations in securing commodity routers, modems, and other network devices. Securing these devices is important as there are serious cybersecurity considerations surrounding the usage of network devices. (https://www.cisecurity.org/insights/white-papers/cis-controls-telework-and-small-office-network-security-guide)

21.4 Learn More

- For more tips on working with vendors, review CIS's "A Guide for Ensuring Security in Election Technology Procurements."

21.5 Mapping to CIS Controls and Safeguards

- 3.10: Encrypt Sensitive Data in Transit (Level 1 maturity)
- 6.3: Require MFA for Externally-Exposed Applications (Level 1 maturity)
- 6.4: Require MFA for Remote Network Access (Level 1 maturity)
- 12.6: Use of Secure Network Management and Communication Protocols (Level 1 maturity)
- 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure (Level 2 maturity)

21.6 Mapping to CIS Handbook Best Practices

- 44, 46, 83

CHAPTER

TWENTYTWO

MANAGING REMOVABLE MEDIA

While removable media such as *USB* drives and *PCMCIA* cards are going extinct in most IT environments, they are still an important tool for environments in which some machines are not network connected.

In the election environment, the election management system and voting systems typically have no network connections and are not on the internet, so removable media remains a part of everyday life.

While keeping hardware and software off of networks can eliminate certain threats, others can be introduced by exchanging data with removable media. Election offices need to be sure to properly source and sanitize anything used to physically transfer data between machines.

22.1 Goals

1. Employ appropriate media sanitization (Level 1 maturity)
2. Effectively use removable media in the election environment (Level 1 maturity)

22.2 Actions

For Managing Removable Media, the necessary actions vary by maturity, as detailed below.

22.2.1 Level 1 Maturity

1. Wherever possible, use removable media only once. This could mean using a *CD-R*, *DVD-R*, or other once-write media, but that can be difficult with today's machines.
2. Instead, use *USB* sticks or other removable media like flash cards.
    - If your budget can sustain it, use them once. If not, follow a media sanitization guide to reduce the risk of introducing *malware* into your non-networked machines.
3. Source your removable media from trusted sources or, if you can't, the consumer market, like a big box store where there's enough volume that it would be difficult to target you as an election office.
    - CIS's cybermarket offers USB sticks and other products from vetted vendors.
4. Regardless of all other guidance, be sure to follow the guidance and directives of their chief election official and voting system vendor.

22.2.2 Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Make removable media sanitization a part of your larger media sanitization program. NIST SP 800-88 is the gold standard for such a program.

22.3 Cost-Effective Tools

- CIS's cybermarket. A buying guide for EI-ISAC members, providing products from trusted vendors at discounted rates.

22.4 Mapping to CIS Controls and Safeguards

- 3.9: Encrypt Data on Removable Media (Level 1 maturity)
- 10.3: Disable Autorun and Autoplay for Removable Media (Level 1 maturity)
- 10.4: Configure Automatic Anti-Malware Scanning of Removable Media (Level 2 maturity)

22.5 Mapping to CIS Handbook Best Practices

- 4, 22, 55, 63

CHAPTER

TWENTYTHREE

MANAGING VENDORS

In nearly all election jurisdictions, many of the hardware, software, and services that underpin our elections—from voter registration and election management systems to pollbooks and vote capture devices—are procured from private vendors.

Even simple public-facing websites may be procured and their security—or lack thereof—may have consequences on elections. The industry partners from which *IT* is procured play a critical role in managing the security risks inherent in elections.

Understanding and properly managing security expectations in the procurement process can have a substantial impact on the success of the election process.

23.1 Goals

1. Understand how to use procurements to achieve security goals (Level 1 maturity)

23.2 Actions

For Managing Vendors, the necessary actions are the same for all maturity levels.

1. Use CIS's A Guide for Ensuring Security in Election Technology Procurements to guide your procurements.

23.3 Cost-Effective Tools

- CIS's A Guide for Ensuring Security in Election Technology Procurements

23.4 Mapping to CIS Controls and Safeguards

- 15.1: Establish and Maintain an Inventory of Service Providers (Level 1 maturity)
- 15.2: Establish and Maintain a Service Provider Management Policy (Level 2 maturity)
- 15.3: Classify Service Providers (Level 2 maturity)
- 15.4: Ensure Service Provider Contracts Include Security Requirements (Level 2 maturity)
- 15.5: Assess Service Providers (Level 3 maturity)
- 15.6: Monitor Service Providers (Level 3 maturity)

- 15.7: Securely Decommission Service Providers (Level 3 maturity)

23.5 Mapping to CIS Handbook Best Practices

- 18, 20, 34, 37, 62, 73

CHAPTER

TWENTYFOUR

MANAGING WIRELESS NETWORKS

Wireless networks are a critical piece of modern connectivity. In the election environment, some systems, like voting machines, are never connected to a wireless network. Others, like e-pollbooks, often have to be to on a wireless network to properly update voter rolls. Some jurisdictions use wireless networks to transmit election results on election night.

There's also the day-to-day administration of the elections that occur on regular workstations used by employees throughout an election office. These may use wired or wireless connections and have access to private networks or the internet.

Good cybersecurity outcomes require proper management of the wireless networks and connections in offices and polling places.

24.1 Goals

1. Protect all wireless networks with basic wireless security practices (Level 1 maturity)
2. Deploy additional tools and measures to limit risk (Level 2 maturity)
3. Deploy mutual MFA for wireless access (Level 3 maturity)

24.2 Actions

For Managing Wireless Networks, the necessary actions vary by maturity as detailed below.

24.2.1 Level 1 Maturity

For those organizations operating at a Level 1 maturity, the important thing is to keep it simple. Avoid using wireless in risky scenarios, such as transmitting election results without the technical support of a state agency or other technical body providing guidance.

1. Use the advanced encryption standard (*AES*) to encrypt wireless data.
2. Create a separate wireless network (a guest network) for personal and untrusted devices.
3. Change administrator passwords on routers and other wireless access points to a secure passphrase.
4. Change the default access passphrase for wireless networks regularly, or enable user level authentication for private networks.
5. Don't permit visitors to use your primary wireless network. Instead set up a guest network.
6. Carefully decide whether a new device will be allowed on the network; you don't need to permit every new device onto the network.

7. Keep firmware and software up to date by including your router and other access points in your *patching* schedule.
8. Track what's on your network.
9. Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (*WPA2*) Enterprise or greater). All wireless access points owned and operated by the jurisdiction should use either *WPA2* or *WPA3* with a strong password.

24.2.2 Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Maintain an inventory of authorized wireless access points to ensure rogue ones are not introduced.
2. Disable wireless access on devices if the device does not strict require wireless connectivity.
3. Disable peer-to-peer wireless network capabilities on wireless clients to prevent communication between devices that is not visible on the wireless network.

24.2.3 Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Use wireless authentication protocols that require mutual, multi-factor authentication.
2. Detect wireless access points connected to the wired network.

24.3 Mapping to CIS Controls and Safeguards

- 12.1: Ensure Network Infrastructure is Up-to-Date (Level 1 maturity)
- 3.10: Encrypt Sensitive Data in Transit (Level 2 maturity)
- 12.3: Securely Manage Network Infrastructure (Level 2 maturity)
- 12.6 Use of Secure Network Management and Communication Protocols (Level 2 maturity)

24.4 Mapping to CIS Handbook Best Practices

- 5, 56

CHAPTER

TWENTYFIVE

NETWORK MONITORING AND INTRUSION DETECTION

Intrusion Detection Systems (*IDSs*) monitor network traffic traveling into and out of networks for malicious activity. These sensors passively monitor network data traffic but do not block traffic and cannot directly affect a member network or change the actual data traversing the network. Other technologies, called Intrusion Prevention Systems (*IPSs*), can also block traffic that the sensors deem a threat.

IDSs monitor traffic as it flows across a network to look for matches against a set of threat signatures. If a match is found, an alert is sent for analysis and, if warranted, further action. In this way, an *IDS* can provide protection against both traditional and advanced network threats by helping organizations identify malicious activity.

The *EI-ISAC* offers an IDS called Albert to election offices. Albert sensors reside on the local network, providing security alerts for cyber threats, helping organizations identify malicious cyber activity. The sensor passively monitors network data traffic; it does not block traffic and cannot negatively affect a member network or read or change the actual data traversing the network.

Under this service, the EI-ISAC receives any alerts, analyzes them, and works with your office to take any recommended action. The EI-ISAC can also be used to analyze historical data to retroactively search for malicious activity. While the Albert sensor is optimized for use in the state, local, tribal, and territorial governments, commercial *IDS* and *IPS* systems are also available.

25.1 Goals

1. Understand what an *IDS* is and why it's important (Level 1 maturity)
2. Deploy an *IDS* (Level 2 maturity)

25.2 Actions

For Network Monitoring and Intrusion Detection, the necessary actions vary by maturity as detailed below.

25.2.1 Level 1 Maturity

We don't recommend investing in an *IDS* at the Level 1 maturity.

While it can provide protection in any network environment, there are more fundamental steps to take, as described in the best practice *prioritization* for Level 1.

25.2.2 Level 2 and Level 3 Maturities

1. Consider investing in an *IDS* or *IPS*.
    - The Albert sensor and service is a free or low-cost way to do this that is optimized for use in the election offices and other state, local, tribal, and territorial governments. Contact elections@cisecurity.org to get information about Albert.

25.3 Mapping to CIS Controls and Safeguards

- 13.3: Deploy a Network Intrusion Detection Solution
- 13.4: Perform Traffic Filtering Between Network Segments
- 13.8: Deploy a Network Intrusion Prevention Solution

25.4 Mapping to CIS Handbook Best Practices

- 7

CHAPTER

TWENTYSIX

PATCHING AND VULNERABILITY MANAGEMENT

Patching is the process of applying available software updates to an operating system, application, browser, mobile app, plugin or other type of software. While patches may bring new and useful functionality, patches are also security updates that address known vulnerabilities that could allow cyber threat actors unauthorized access to information systems or networks. While there are some differences, for the purposes of this guide, patching and vulnerability management are synonymous.

Unpatched vulnerabilities remain one of the primary infection vectors observed by the *EI-ISAC* and our partners. Once patches are publicly announced, information on the associated vulnerabilities they remediate is generally available to anyone, including cyber threat actors. This significantly increases the likelihood that the threat actors will attempt to exploit unpatched systems using information deduced from the patch release.

Software development companies, such as Microsoft and Adobe, regularly release bulk security patches for their products on the second Tuesday of every month, which is known as Patch Tuesday. Other companies release patches on other days of the month, quarterly, or on an ad hoc basis. In the U.S., most publicly known cybersecurity vulnerabilities are cataloged in the National Vulnerability Database (*NVD*) maintained by *NIST*. Each vulnerability in the patch is rated based on the associated level of risk, threat, and impact, along with other factors. The NVD frequently asked questions provide a wealth of information on the NVD.

Successful exploitation of unpatched election infrastructure may result in data breaches, malware infections, and website defacements, among other things. Information at risk includes personally identifiable information (*PII*) and other voter information.

The *MS-ISAC* regularly disseminates Cybersecurity Advisories, which address critical patches in commercial software commonly used by government agencies and are available to all *EI-ISAC* members. To subscribe to Cybersecurity Advisories, *EI-ISAC* members should contact their account manager or complete the subscription form.

26.1 Goals

1. Understand the importance of patching (Level 1 maturity)
2. Establish a patching schedules (Level 1 maturity)
3. Establish and execute on a policy for systems that need additional approvals prior to patching (Level 1 maturity)
4. Establish a formal patch management plan leveraging automated tools and aligned with your asset management plan (Level 2 maturity)

26.2 Actions

For Patching and Vulnerability Management, the necessary actions vary by maturity as detailed below.

26.2.1 Level 1 Maturity

At the Level 1 maturity, organizations should simply begin patching their systems in a thoughtful and consistent manner.

Not all systems used in elections can be patched immediately. Particularly when patching voting systems, be sure to consider your state's or the U.S. Election Assistance Commission's (*EAC*) System Certification Process and account for scheduled primary and election day system configuration freezes.

1. Verify that all software used in the office is supported by an active development company. If not, update or replace the software. Only download patches from authoritative sources.
2. Patch all operating systems on a regular timetable.
    - It's usually best to patch your operating systems first, and then move to your software applications. Systems should be set to update by automatically.
    - Network devices also need to receive software updates, but this may require a consultation with IT staff or contractors before it's agreed to patch these devices.
    - Devices and applications will often make patches available via a diagnostic menu or administrative console. Each device or application will be different, and this may require some research.
3. Patch all software applications on a regular timetable.
4. Where complex or mission critical systems are used, test and verify patches before patching production systems.

26.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Use automated tools to conduct software patching of your systems.
2. Establish a formal, written plan in place that references the organization's vulnerability management program, as identifying and remediating vulnerabilities goes hand-in-hand with updating software.
    - When creating a patch management program for your office, begin by understanding all the hardware and software assets that you are responsible for by conducting *Asset Management*. Then implement a conssistent process that:
        - Readily identifies patches as they become available.
        - Prioritizes patches for known vulnerable systems.
        - Downloads patches from authoritative sources.
        - Tests and verifies patches in the operating environment.
        - Applies appropriately tested patches to vulnerable systems.

For more comprehensive recommendations and technical insight on this topic, please see the MS-ISAC's Technical White Paper Timely Patching Reduces System Compromises.

26.3 Cost-Effective Tools

- Itarian: Patch management solution for Windows
- Opsi: A more complicated solution that can help to manage both Windows and Linux platforms
- OpenVAS: Free, open-source framework for vulnerability scanning and management

26.4 Learn More

- The MS-ISAC's Technical White Paper Timely Patching Reduces System Compromises
- Apple Auto-update - iOS
- Apple Auto-update - MacOS
- Auto-update Windows
- Auto-update MS Office on macOS
- Auto-update Android

26.5 Mapping to CIS Controls and Safeguards

- 2.2: Ensure Authorized Software is Currently Supported
- 7.3: Perform Automated Operating System Patch Management
- 7.4: Perform Automated Application Patch Management

26.6 Mapping to CIS Handbook Best Practices

- 43, 44, 76

CHAPTER

TWENTYSEVEN

PUBLIC-FACING NETWORK SCANNING

All code needs to be tested for flaws, and given the types of attacks that work on a given type of code change as threat actors develop new techniques, deployed code needs to be tested regularly for known vulnerabilities.

For public-facing assets, various types of scanning can find known vulnerabilities and provide reports that prioritize them based on standardized severities. These scanning tools are automated and can run regularly to always keep you informed of your progress and any new issues due to changes you make or the evolving threat environment.

Common types of scanning or network testing include:

- Vulnerability Scanning: Reviews public-facing websites for vulnerabilities.
- Web application scanning: Reviews public-facing applications for vulnerabilities.
- Remote penetration testing: A more advanced method of using known tactics to simulate attacks and find more difficult to exploit vulnerabilities.

27.1 Goals

1. Deploy scanning tools on your public-facing assets (Level 1 maturity)
2. Deploy web application scanning tools (Level 1 maturity)
3. Use penetration testing to harden networks (Level 2 maturity)

27.2 Actions

For Public-Facing Network Scanning, the necessary actions vary by maturity as detailed below.

27.2.1 Level 1 Maturity

1. Use free tools and services to conduct scans of your publicly-facing assets. This should include your website and any online portals you are responsible for that are used for elections purposes. *CISA* offers all of its cybersecurity assessment services at no cost to election offices.
    - Sign up for free vulnerability scanning by contacting CISA at vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services."
    - If you have web applications, sign up for free web application scanning at vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services."
2. Remediate any vulnerabilities or known issues found during the scans.

Note that scanning online systems you do not own may run afoul of the Computer Fraud and Abuse Act of 1986 (*CFAA*).

27.2.2 Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Implement remote penetration testing.
    - Sign up for free remote penetration testing by contacting *CISA* at vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services."
2. Sign up for the EI-ISAC's Vulnerability Disclosure Program to allow the wide-ranging talent of security researchers to improve the security of your systems.

27.3 Cost-Effective Tools

- CISA Cyber Hygiene Services: CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Types of scans and assessments include vulnerability scanning, web application scanning, phishing campaign assessments, and remote penetration testing.
- ShieldsUP!: ShieldsUP is an online port scanning service that can alert the users of any ports that have been opened through their firewalls or through their NAT routers, which can be used by malicious users to take advantage of security vulnerabilities.

27.4 Mapping to CIS Controls and Safeguards

- 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- 7.7: Remediate Detected Vulnerabilities

27.5 Mapping to CIS Handbook Best Practices

- 2, 19

CHAPTER

TWENTYEIGHT

USER MANAGEMENT

Some of the most commonly exploited vulnerabilities are those that take place where the user meets the machine. User accounts get hijacked and are used to access resources, sometimes methodically over time, to access valuable resources or cause damage.

To reduce the risk of user account incidents, you need to implement strong protections on every user account and limit the amount of damage that may be caused by takeover of a single user account.

1. Passwords: Like it or not, passwords are a reality of online life and will be for some time to come. They are also a common vector of attack by threat actors. You can't have good user management without good password policies.
2. *Multi-factor authentication* (MFA): The best way to address weaknesses in *authentication* is to have the right MFA requirements in place–those that, through a variety of means, use at least two of something you know (like a password), something you have (like a cell phone), and something you are (like a fingerprint) to log in.
3. User accounts: How you manage user accounts–creating, managing, tracking, and deleting–can have a huge impact on your overall cybersecurity posture.

28.1 Goals

1. Implement good password practices (Level 1 maturity)
2. Implement *MFA* wherever possible (Level 1 maturity)
3. Ban or limit shared or generic accounts (Level 1 maturity)
4. Employ least privilege, especially with administrative access, and revoke access appropriately (Level 1 maturity)
5. Log user activity (Level 1 maturity)

28.2 Actions

For User Management, the necessary actions vary by maturity as detailed below.

28.2.1 Level 1 Maturity

User Recommendations

1. Do not reuse passwords across multiple platforms, systems, or software. This includes never using the same login credentials for work and personal use.
2. Never use personal information, such as your name, children's names, dates of birth, etc., that someone might already know or can easily obtain.
3. Use passphrases, ideally of at least four words of 5+ letters, instead of random sets of characters. If you do this, you don't need to use composition rules like upper, lower, number, and symbols. An example of a good passphrase is "blender saute pendant chair."
4. Use a password manager, and protect access to it with MFA.

Organizational Recommendations

1. Remove all default accounts or change the default password on all accounts, applications, and systems.
2. Enable MFA anywhere it's offered, on all accounts, for all applications. This is especially true for anything accessed outside your environment, including social media accounts, and any access back into your environment from outside. Ensure this is true for all IT products supplied by vendors.
3. Store all passwords and passphrases using *salting* and *hashing* functions and **not** with reversible *encryption*. Make sure your vendors do the same.
4. Set login thresholds to 10 or fewer invalid login attempts before locking the user out and increase the interval between a failed attempt and allowing the next attempt. Log and monitor all login attempts.
5. Ban or limit shared or generic accounts. In some environments, like with an e-pollbook, it might not be possible or practical to do this. Instead, rotate passwords, passcodes, and biometrics (like TouchID) when reasonable, like with each election.
6. Employ least privilege by only giving a user access to the devices, applications, and services they need to do their jobs. This limits the damage that may be caused by takeover of any single account. This is particularly important for any account with administrative access to sensitive network controls or confidential materials.
7. Review individuals' access and revoke any unnecessary or inappropriate access. Establish a plan to do this regularly, and make it part of the offboarding and job change processes to ensure that user has access to what they need and nothing else.
8. Employ user logging on your networks. You should be able to see whenever a user logs into a device or network. Maintain records of these logs.
9. Allow and encourage use of password managers.

28.2.2 Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Complete all of the actions for the Level 1 maturity.
2. Review *MS-ISAC's* Security Primers on Exposed Credentials and Securing Login Credentials, as well as the United States Computer Emergency Readiness Team's (*US-CERT's*) Security Tip on Choosing and Protecting Passwords.

3. The *EI-ISAC* regularly monitors the Internet for stolen credentials using open source datasets from various security organizations and researchers, as well as information received from trusted partners. To subscribe to this service, simply provide your IP addresses and domains to soc@cisecurity.org.
4. Use services to search for breaches of your users' email addresses and passwords.

28.3 Learn More

- Get more password guidance from *NIST*: SP 800-63B Section 5.1.1.2
- Password spotlight (This spotlight has some out-of-date recommendations. Use in conjunction with the NIST guidance)
- Understand the logic behind using passphrases.

28.4 Mapping to CIS Controls and Safeguards

- 4.7: Manage Default Accounts on Enterprise Assets and Software (Level 1 maturity)
- 5.1: Establish and Maintain an Inventory of Accounts (Level 1 maturity)
- 5.2: Use Unique Passwords (Level 1 maturity)
- 5.3: Disable Dormant Accounts (Level 1 maturity)
- 5.5: Establish and Maintain an Inventory of Service Accounts (Level 2 maturity)
- 5.6: Centralize Account Management (Level 2 maturity)
- 6.1: Establish an Access Granting Process (Level 1 maturity)
- 6.2: Establish an Access Revoking Process (Level 1 maturity)
- 6.3: Require MFA for Externally-Exposed Applications (Level 1 maturity)
- 6.4: Require MFA for Remote Network Access (Level 1 maturity)
- 6.5: Require MFA for Administrative Access (Level 1 maturity)
- 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems (Level 2 maturity)
- 6.7: Centralize Access Control (Level 2 maturity)
- 6.8: Define and Maintain Role-Based Access Control (Level 2 maturity)

28.5 Mapping to CIS Handbook Best Practices

- 24, 25, 26, 47, 49, 50, 51, 52, 66, 77, 78, 81

CHAPTER

TWENTYNINE

WEBSITE SECURITY

An election office's website is often the first and most important source of information for voters, the media, and other interested parties. It is extremely important to have a secure website that is resistant to attacks and provides critical information with an official, professional manner and appearance.

29.1 Introduction

This best practice covers five important topics about websites, as detailed below.

29.1.1 The .gov top-level domain

Top-level domains are important to understand both from a cybersecurity perspective and to know how constituents will engage with and access your web presence. The ".gov" domain suffix is restricted to verified U.S. government entities, which helps ensure legitimacy for visitors browsing U.S. government websites. Additionally, ".gov" domain owners are required to maintain a higher level of security, and the federal government has implemented several cybersecurity controls in the underlying infrastructure.

As .gov domains are carefully controlled, once you have one you can communicate to your constituents that they should only trust a .gov for official information.

29.1.2 Securing a site with HTTPS

Hyper Text Transfer Protocol Secure (HTTPS) is an internet communication protocol used to encrypt and securely transmit information between a user's web browser and the website they are connected to. HTTPS accomplishes this through the use of a Secure Sockets Layer (SSL) certificate, which establishes an encrypted connection. The certificate also helps authenticate that the website and the user are who they say they are when communicating.

HTTPS is the norm across the internet. Major web browsers label websites that do not use HTTPS as "not secure" and often require users to take additional steps to visit the site. Even if the site doesn't contain malicious content, this can dissuade people from trusting your official site.

29.1.3 Denial of service attacks

A denial of service attack (DoS) seeks to disrupt the availability of a system or service. Additionally, threat actors may use multiple source computers in a distributed denial of service (DDoS) attack.

Typically, these attacks target webservers in order to overwhelm the webserver's internet connection or its ability to respond to user requests. If the threat actors can send more requests than permitted by the system, the webserver or internet connection will be too busy to respond to additional requests, resulting in a "denial of service" to legitimate users. Of note, computers participating in a DDoS attack may be infected with malware that conducts the attack, which means they are also victims of malicious activity.

29.1.4 Typosquatting

Typosquatting attempts to take advantage of errors users might make when URLs are typed directly into the address bar. Similarly, malicious actors may seek to trick users into taking a quick glance at a URL and opening a visually similar yet malicious link.

29.1.5 Website defacements

Website defacements are the unauthorized modification of web pages, including the addition, removal, or alteration of existing content. Websites that are unpatched or misconfigured are easily susceptible to simple probing tools used by these actors, which can lead to unauthorized access to websites.

While in most cases they seem to be simply a nuisance, website defacements pose a potential public relations concern for election offices and could promote disinformation, including the alteration of time and dates for open voting events or unofficial results. These changes may be subtle and thus difficult to detect.

29.2 Goals

1. Move your website to the .gov top-level domain (Level 1 maturity)
2. Use HTTPS everywhere (Level 1 maturity)
3. Prevent denial of service attacks (Level 1 maturity)
4. Understand typosquatting and what to do about it (Level 1 maturity)
5. Know about website defacements and how to prevent them (Level 1 maturity)
6. Enroll in the EI-ISAC's vulnerability disclosure program (Level 2 maturity)

29.3 Actions

For Website Security, the necessary actions vary by maturity as detailed below.

29.3.1 Level 1 Maturity

1. Visit https://dotgov.gov to sign up for and manage a .gov website and email domain.
    - Effectively managing a website can be difficult, but the good news is that you can mitigate many of the risks with one simple step: getting a .gov domain. A .gov domain automatically provides HTTPS and reduces the likelihood of your constituents confusing other websites for yours.
2. Stop denial-of-service (DOS) attacks by using no-cost tools.
    - Tools, including those from from Cloudflare and Google, will mitigate instances of these attacks.
    - Learn more through the EI-ISAC's Guide to DDoS Attacks.
3. Reduce the risk of typosquatting by:
    - Communicating that your .gov site is the only official site.
    - Register or purchase variations of your domain, such as your domain but with .com, .org, and .net addresses and common typos that might occur.
4. Manage website defacements by:
    - Developing a plan to defend against and recover from website defacements.
        - Consider temporarily pulling down the site to prevent any further misrepresentation.
        - Have a recovery plan created on how to alert readers about the targeted website.
        - Have offline *backups* established that can be quickly deployed in place of a compromised website.
    - Maintain *up-to-date software and patch vulnerabilities*.
    - Enroll in CISA's CyHy program or the EI-ISAC's Vulnerability Assessment to receive notifications on outdated software.

29.3.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Establish a vulnerability management program (*VDP*): A VDP is a formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems.
    - By working with external security researchers, organizations can broaden their vulnerability management efforts and remake them as a continuous process—all while saving time and money.
    - The EI-ISAC offers a VDP that makes it easier for election offices to create and operate a VDP. Contact elections-vdp@cisecurity.org for more information.

29.4 Cost-Effective Tools

- DotGov.gov: The government portal to obtain and manage a .gov domain.
- CyHy program: CISA's cyber hygiene web application scanning program.
- Cloudflare's Athenian Project: Free security and performance for state and local election websites.
- Google's Project Shield: A free service that defends news, human rights and election monitoring sites from DDoS attacks.

29.5 Learn More

- Election Security Spotlight – Typosquatting

29.6 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls

29.7 Mapping to CIS Handbook Best Practices

- 9

CHAPTER

THIRTY

INDEX OF APPENDICES

The Essential Guide to Election Security includes several appendices to provide additional information that may be helpful to users.

The appendices are:

1. *About the Guide*: Information about the structure of the document, its history, and its relevance to CIS's Handbook for Election Infrastructure Security.
2. *How To*: Information on the best uses and most effective ways to work with the Guide to achieve that which you wish to accomplish.
3. *Acronyms*: Expansions of acronyms used in the Guide.
4. Small Jurisdiction *Worksheets*: A set of downloadable worksheets for use at the Level 1 maturity level.
5. For legacy purposes, a *mapping* of the best practices to the best practices from the Handbook for Election Infrastructure Security.

In addition, there is a *glossary* of technical terms used throughout the Guide.

CHAPTER

THIRTYONE

ABOUT THE ESSENTIAL GUIDE TO ELECTION SECURITY

When The Handbook for Election Infrastructure Security was published in 2018, election officials had much less guidance to rely on. Today, they often have the opposite problem: an enormous amount of guidance to navigate. With so much guidance and so many tools and approaches available, it's difficult for any given election official to know what will best work for them.

This Guide aims to solve that problem and aid the process of building a program designed to meet the individual needs and abilities of any given election office.

31.1 Why does this Guide look like a webpage? (Or does it??)

You might be reading this online. Or you might be reading a PDF. If the latter, it's because your PDF was built from an online version. Here's why we're keeping all of the content for the Guide online:

CIS published The Handbook for Election Infrastructure Security in early 2018, just before the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) launch.

In 2021, the EI-ISAC began working with the election community to update that Handbook. A common item of feedback we received was that the static nature of the Handbook meant it didn't include any of new and evolving the best practices that weren't already in place in early 2018.

Creating an updated version of that Handbook would've left us in the same position: the pace of new best practices and services available to secure election infrastructure is too rapid to rely on a static model for communicating them to election officials.

Instead, we decided to create this dynamic, always up-to-date online Guide. It can still be exported as one big PDF, but when you do so, you will get the best practices current as of the moment you hit the button to create the PDF.

We can also embed and link to more engaging content like videos and examples. When best practices change, officials face new risks, or different resources become available, we can quickly update the Guide to reflect the new state of the world.

31.2 What's Changed

Election offices operate in an environment heavy on information technology (*IT*). The teams administering elections have been protecting these environments for decades. Still, as the threats evolve and the measures for mitigating IT risk increase in complexity, their task becomes ever more difficult.

In early 2018, *CIS*, with significant contributions from the election community, published its Handbook for Election Infrastructure Security, a guide to assist election offices in defending their IT systems from cybersecurity threat actors. It consisted of 88 best practices to mitigate risk across all types of election equipment.

The EI-ISAC received positive feedback from the election community on the Handbook's value. In the four years since then, several significant changes have occurred:

1. The CIS Controls, on which many of the 88 best practices are based, underwent a major revision.
2. The Election Infrastructure Information Sharing and Analysis Center (*EI-ISAC*) has greatly increased the number of freely available tools and services for election offices across the country.
3. Since releasing the Handbook, the EI-ISAC has developed a series of best practice guides and other information. Other organizations have also contributed to the body of knowledge for security election infrastructure and related activities, including:
    - A wide array of guidance and tools available from the Cybersecurity and Infrastructure Security Agency (*CISA*) and other government agencies; and
    - A body of work for other academic and nonprofit organizations such as the Global Cyber Alliance, Harvard University's Belfer Center, the Brennan Center for Justice, and others.
4. Election officials have made significant strides in meeting today's threats, but uneven and insufficient funding has caused a wide array of differences in cybersecurity postures.
5. The nature of threats has changed. In 2016, nation-state actors posed most of the apparent risks. Today we have more information on real-world attacks. We know that they come various sources and come from both virtual and real-life sources.
6. Mis-, dis-, and mal-information (*MDM*) has become one of the thorniest and most pervasive threats to democracy and election officials need guidance on mitigating misinformation and threats and harassment of election officials. This includes many types of MDM, including about the administration of a specific election, issue- and candidate-based, and delegitimization of election results.

31.3 How is this version different?

These changes to the election ecosystem warrant a rethinking of the original Handbook. Developed in collaboration with federal partners, state and local election officials, and election technology providers, this update takes several major steps to address this continual evolution of the election space:

1. We've developed a more rigorous maturity model. The original Handbook simply listed high, medium and low priorities for each of the 88 best practices. This gave a rough order in which to implement best practices, but didn't account for a given jurisdiction's resources or capabilities. We now have three maturities and a decision tree for finding an organization's fit. For any best practice, the approach to implementation addresses whether, for instance, the office has limited technical expertise or well-trained teams of IT security specialists. These are described in detail in the *Maturities* section.
2. We've incorporated new best practices that cover the many threats and opportunities that have emerged, like around managing mis-, dis- and mal-information (*MDM*) and free services. We'll continue adding and evolving guidance as necessary.
3. For each best practice, we've provided more information on what actions to take and how to get the job done, so even readers with the least technical knowledge know how to get started.
4. We've added a substantial listing of available resources and additional direction throughout the best practices.
5. We've moved from the original Handbook—a static paper or PDF document—to a more dynamic web-based experience. As described *earlier*, this allows continually updated online tools, videos, and resources as threats evolve and new opportunities emerge.
6. We're developing a "peer support" tool to enable election teams to communicate with each other, creatively solve problems, share best practices, and rapidly and collaboratively respond to emerging issues. Expect to see this later in 2022.

In addition to these, there are many minor updates we hope improve the usability of this Guide, allowing it to serve as an effective tool for every election office regardless of size, resources, or technical sophistication.

31.4 We Love Feedback

We'll take feedback at any time. Provide feedback 1 of 2 ways:

1. Send any feedback to essentialguide@cisecurity.org. You can export a PDF (hover over "v:latest" in the bottom left and hit "PDF") and comments directly in it. You can also put feedback directly in the email.
2. If you're familiar with GitHub, we'd love to get feedback through issues and pull requests. You can get to the repo through the menu in the bottom left of any Read The Docs page (hover over "v:latest" and hit "view" under "On Github"). Feel free to fork the repo and create a PR when you're ready, or directly add issues to the repo with the tag "community review."

Thank you!

CHAPTER

THIRTYTWO

HOW TO USE THE ESSENTIAL GUIDE TO ELECTION SECURITY

You can navigate the document online by using the navigation panel at the left or the previous and next links at the bottom of each page.

You can create a PDF by hovering over the “v:latest” in the bottom left, at the bottom of the navigation panel. The box that pops up will have a “PDF” link. Hit that link and you’ll get a PDF based on the current version of the Guide.

CHAPTER

THIRTYTHREE

ACRONYMS

NIST's Computer Security Resource Center Glossary is a useful reference for information security terms, acronyms, and organizations.

AES Advanced Encryption Standard

CDM *Community Defense Model*

Continuous Diagnostics and Mitigation

Continuous Diagnostics and Monitoring

CD-R Compact Disc Read-only

CFAA Computer Fraud and Abuse Act of 1986

CIS Center for Internet Security

CISA Cybersecurity and Infrastructure Security Agency

NIST CSF NIST Cybersecurity Frameowrk

CVE *Common Vulnerabilities and Exploits*

DNS Domain name system

DVD-R Digital Video Disc Read-only

EAC Election Assistance Commission

EDR *Endpoint Detection and Response*

EI-ISAC Election Infrastructure Information Sharing and Analysis Center

EMS Election Management System

IDS Intrusion Detection System

IG Implementation Group

IPS Intrustion Prevention System

IT Information Technology

MDBR *Malicious Domain Blocking and Reporting*

MDM Mobile Device Management OR

Mis-, Dis-, and Mal-Information

MFA *multi-factor authentication*

MS-ISAC Multi-State Information Sharing and Analysis Center

NCSR National Cybersecurity Review

NIST National Institute of Standards and Technology

NIST SP NIST Special Publication

NVD National Vulnerability Database

PCMCIA Personal Computer Memory Card International Association

PII Personally-Identifiable Information

US-CERT United States Computer Emergency Readiness Team

USB Universal Serial Bus

VDP Vulnerability Disclosure Program

VPN Virtual Private Network

WPA Wi-Fi Protected Access

CHAPTER

THIRTYFOUR

LEVEL 1 WORKSHEETS

This page links to a set of worksheets for use at the Level 1 maturity level. There is one Excel format file to download that contains all ten worksheets.

Completing these worksheets provides the *baseline priorities* for Level 1.

A organization at the Level 1 maturity should still complete the Level 1 *election priorities*.

There are ten total worksheets in one file. Download the full set of worksheets in Excel format.

34.1 IT Inventory Worksheets

Within the Excel format download, the first five worksheets are about *IT* Inventory. Each is simple and, together, should only take a few hours to complete for a small office. These fulfill action #1 of the *Asset Management* best practice for the Level 1 maturity.

1. Hardware asset inventory
2. Software asset inventory
3. Service provider inventory
4. Account inventory
5. Data inventory

34.2 Cybersecurity Action Worksheets

Within the Excel format download, the last five worksheets are about taking action on cybersecurity in your office. Each is simple and, together, should only take a few hours to complete for a small office. These fulfill the remainder of the Level 1 maturity, as described in the Level 1 *election priorities*.

1. Asset protection
2. Account security
3. Backup & recovery
4. Incident response
5. Cyber education

CHAPTER

THIRTYFIVE

MAPPING TO THE HANDBOOK FOR ELECTION INFRASTRUCTURE SECURITY

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
1	Whitelist which IPs can access the device	
2	Regularly scan the network to ensure only authorized devices are connected	Public-Facing Network Scanning
3	Limit the devices that are on the same subnet to only those devices required	
4	Only utilize approved and managed USB devices with appropriate device encryption and device authentication	• Encrypt Data at Rest • Removable Media
5	Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials	Managing Wireless Networks
6	Ensure the system is segregated from other independent election systems and non- election supporting systems	
7	Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on internet and extranet DMZ systems	Network Monitoring and Intrusion Detection
8	If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)	
9	Use trusted certificates for any publicly- facing website	Website Security
10	Ensure logs are securely archived	
11	On a regular basis, review logs to identify anomalies or abnormal events	

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
12	Ensure critical data are encrypted and digitally signed	Encrypt Data at Rest
13	Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines	Building and Managing Staff
14	Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing	
15	Ensure acceptance testing is done when receiving or installing new/updated software or new devices	
16	Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process	Building and Managing Staff
17	Deploy application whitelisting	
18	Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards	Managing Vendors
19	Regularly run a SCAP-compliant vulnerability scanner	Public-Facing Network Scanning
20	Utilize EAC certified or equivalent software and hardware products where applicable	Managing Vendors
21	Store secure baseline configuration on hardened offline system and securely deploy baseline configurations	Backups
22	Utilize write once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.	Removable Media
23	Maintain detailed maintenance record of all system components	• Asset Management • Managing Infrastructure
24	Require the use of multi-factor authentication	User Management

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
25	Require users to use strong passwords (14 character passphrases) if multi factor authentication is not available	User Management
26	Limit the number of individuals with administrative access to the platform and remove default credentials	User Management
27	Ensure that all devices are documented and accounted for throughout their lifecycle	• Asset Management • Managing Infrastructure
28	Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible	Asset Management
29	Maintain an inventory of assets that should be on the same subnet as the election system component	
30	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Asset Management
31	Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks	
32	Limit the use of personally identifiable information. When it is required, ensure that that it is properly secured and staff with access are properly trained on how to handle it.	Endpoint Protection
33	Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas	Exercising Plans
34	Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities	Managing Vendors
35	Implement a change freeze prior to peak election periods for major elections	
36	Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures	
37	Work with vendors to establish and follow hardening guidance for their applications	Managing Vendors

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
38	Ensure logging is enabled on the system	
39	Use automated tools to assist in log management and where possible ensure logs are sent to a remote system	
40	Where feasible, utilize anti-malware software with centralized reporting	Endpoint Protection
41	Ensure only required ports are open on the system through regular port scans	Firewalls and Port Restrictions
42	Where feasible, implement host-based firewalls or port filtering tools	Firewalls and Port Restrictions
43	Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available	Software Updates
44	Ensure vendors distribute software packages and updates using secure protocols	• Managing Remote Connections • Software Updates
45	Maintain a chain of custody for all core devices	Asset Management
46	All remote connection to the system will use secure protocols (TLS, IPSEC)	Managing Remote Connections
47	Users will use unique user IDs	User Management
48	Use a dedicated machine for administrative tasks to separate day to day functions from other security critical functions (For some components this may not be practical to implement)	
49	Ensure that user activity is logged and monitored for abnormal activities	User Management
50	Regularly review all accounts and disable any account that can't be associated with a process or owner	User Management
51	Establish a process for revoking system access immediately upon termination of employee or contractor	User Management
52	Ensure that user credentials are encrypted or hashed on all platforms	User Management
53	Ensure all workstations and user accounts are logged off after a period of inactivity	

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
54	Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system	Building and Managing Staff
55	For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging	• Asset Management • Removable Media
56	Disable wireless peripheral access of devices	Managing Wireless Networks
57	Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines	Building and Managing Staff
58	Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process	Building and Managing Staff
59	Ensure staff is properly trained for reconciliation procedures for the pollbooks to the voting systems and reconcile every polling place and voter record in accordance with local, state, and federal guidelines	Building and Managing Staff
60	Store secure baseline configuration on hardened offline system and securely deploy baseline configurations	Backups
61	Work with the vendor to deploy application whitelisting	
62	Utilize the most up-to-date and certified version of vendor software	Managing Vendors
63	Utilize write once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.	Removable Media
64	Only use the devices for election related activities	
65	Maintain detailed maintenance records of all system components	• Asset Management • Managing Infrastructure
66	Limit the number of individuals with administrative access to the platform and remove default credentials	User Management

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
67	Utilize tamper evident seals on all external ports that are not required for use	Asset Management
68	Ensure that all devices are documented and accounted for throughout their lifecycle	• Asset Management • Managing Infrastructure
69	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Asset Management
70	Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing	
71	Ensure acceptance testing is done when receiving or installing new or updated software or new devices	
72	Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas	Exercising Plans
73	**Identify and maintain information on network** service providers and third-party companies contacts with a role in supporting election activities	• Incident Response • Managing Vendors
74	Implement a change freeze prior to peak election periods for major elections	
75	Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures	
76	Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available	Software Updates
77	Ensure the use of unique user IDs	User Management
78	Ensure individuals are only given access to the devices they need for their job	User Management
79	Maintain a chain of custody for all core devices	Asset Management
80	Ensure all workstations and user accounts are logged off after a period of inactivity	

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
81	Regularly review all authorized individuals and disable any account that can't be associated with a process or owner	User Management
82	Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system	Building and Managing Staff
83	Use secure protocols for all remote connections to the system (TLS, IPSEC)	Managing Remote Connections
84	Ensure critical data is encrypted and digitally signed	Encrypt Data at Rest
85	Ensure the use of bidirectional authentication to establish trust between the sender and receiver	
86	For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging	Asset Management
87	Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process	Building and Managing Staff
88	Track all hardware assets used for transferring data throughout their lifecycle	• Asset Management • Managing Infrastructure

CHAPTER

THIRTYSIX

GLOSSARY

NIST's Computer Security Resource Center Glossary is a useful reference for information security terms, acronyms, and organizations.

authentication Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

CIS Controls A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks

common vulnerabilities and exploits The generic name for known cybersecurity vulnerabilities that have been catalogued by the CVE program. There is one CVE Record for each vulnerability in the catalog.

Community Defense Model A set or real-world analyses used to design, prioritize, implement, and improve an enterprise's cybersecurity program. See the CDM 2.0 release.

disinformation Information deliberately created to mislead, harm, or manipulate a person, social group, organization, or country

domain name system The system by which Internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs.

encryption Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data

Endpoint Detection and Response Security software that is deployed on workstations and servers, to collect technical data and analyze it for suspicious patterns and threats.

Endpoint Protection Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.)

hashing The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data

Implementation Group The recommended guidance to prioritize implementation of the CIS Critical Security Controls (CIS Controls). They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls.

malinformation Information based on fact, but used out of context to mislead, harm, or manipulate

malicious domain blocking and reporting Technology that prevents *IT* systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats

malware Malware is malicious software or software designed to perform malicious actions on a device. It can be introduced to a system in various forms, such as emails or malicious websites.

misinformation Information that is false but not created or shared with the intention of causing harm

multi-factor authentication An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

patching The act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities

ransomware A type of malware that blocks access to a system, device, or file until a ransom is paid

salting A non-secret value used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker

virtual private network Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line

INDEX

