CIS Center for Internet Security®

Creating Confidence in the Connected World.™

The Essential Guide to Election Security

Release 1.5.0

INTRODUCTION

1 The Essential Guide to Election Security 1

2 Maturities 4

3 Determining Your Maturity Level 6

4 Prioritizing Best Practices for the Level 1 maturity 9

5 Prioritizing Best Practices for the Level 2 and Level 3 maturities 12

6 Index of Best Practices 16

7 Addressing Physical Threats 18

8 Join the MS-ISAC 21

9 Asset Management 23

10 Encrypt Data at Rest 27

11 Encrypt Data in Transit 30

12 Managing Infrastructure with Secure Configurations 33

13 User Management 36

14 Backups 41

15 Incident Response Planning 45

16 Building and Managing Staff 48

17 Patching and Vulnerability Management 50

18 Remediate Penetration Test Findings 55

19 Perform Internal Penetration Test 58

20 Network Segmentation Based on Sensitivity 60

21 Managing Remote Connections 62

22 Firewalls and Port Restrictions 65

23 Endpoint Protection 68

24 Malicious Domain Blocking and Reporting 71

25 Network Monitoring and Intrusion Detection 74

26 Managing Wireless Networks 77

27 Public-Facing Network Scanning 80

28 Website Security 83

29 Managing Removable Media 87

30 Exercising Plans 89

31 Formal Cybersecurity Assessments 91

32 Implementing the CIS Controls 94

33 Managing Inaccurate Election Information 97

34 Managing Vendors 100

35 Defense-in-Depth 102

36 Artificial Intelligence in Elections 105

37 Preparing for Election Day Disruptions 108

38 Index of Appendices 113

39 About the Essential Guide to Election Security 114

40 How to Use the Essential Guide to Election Security 118

41 Level 1 Worksheets 119

42 Mapping to the Handbook for Election Infrastructure Security 121

43 A Primer on Election Infrastructure Security 130

44 Election Systems and Their Network Connections 132

45 Voter Registration 134

46 Pollbooks 138

47 State and Local Election Management Systems 141

48 Vote Capture 143

49 Vote Tabulation 147

50 Election Results Reporting and Publishing 149

51 Glossary 151

52 Acronyms 153

Index 155

CHAPTER

ONE

THE ESSENTIAL GUIDE TO ELECTION SECURITY

Want to skip straight to the action?

- Determine your *maturity level* (page 6)
- See the Level 1 maturity *best practices* (page 9) and the Level 2 and Level 3 maturities *best practices* (page 12)
- For a true beginner, read our *primer* (page 130) on election infrastructure security for an introduction into the types of systems used in election administration and the risks and threats associated with them.

To first learn more, read on…

1.1 A Best Practices Resource for Election Professionals

The Center for Internet Security[1] (*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* (page 114) appendix.

[1] https://cisecurity.org

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 Structure of this Guide

The Guide is organized into several sections:

1. An introduction.
2. A description of *maturities* (page 4) and how they are used in the document.
    - Maturities are used to reflect an organization's capabilities in managing cybersecurity risk
    - Best practices and actions are prioritized based on maturity, so knowing your maturity is important to chart your path through the rest of the Guide.
3. A set of *best practices* (page 16) for organizations to implement.
    - Each best practice has an introduction to the topic as well as goals and actions for each maturity level.
    - There are also lists of cost-effective tools, additional resources, and mappings to the CIS Controls.
    - There is a mapping to best practices from the Handbook for Election Infrastructure Security, the predecessor to this Guide. Find a full mapping *here* (page 121).
    - There is also a set of worksheets you can download if you are at the Level 1 maturity and need to complete the *baseline priority* (page 10) best practices.
    - The best practices are ordered as follows:
        1. Addressing physical threats: First, be safe. Then be cybersecure.
        2. Join the MS-ISAC: Becoming a member gives you free access to many of the tools in the rest of the best practices.

    3. Baseline priority best practices for the Level 1 maturity: most of the actions within these best practices are supported with the worksheets described above. See the Level 1 maturity the *baseline priority* (page 10) best practices.

    4. Priority based on CIS's Community Defense Model 2.0. See *the top priority safeguards mapped to the best practices* (page 12).

4. Additional references, tools, and related information in *appendices* (page 113).

5. A *glossary* (page 151) and set of *acronyms* (page 153).

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.

Find more detailed information on this Guide and how to use it in our *how to* (page 118).

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.

This guide in a continual development process, and CIS is interested in feedback from all readers. Ideas for content and usability improvements are most welcome, as are any questions if you find yourself with a question or needing more help. Always feel free to reach out to the MS-ISAC team at info@msisac.org. We also encourage you to use trusted partners and peers at the federal, state, and local levels for guidance and support.

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.

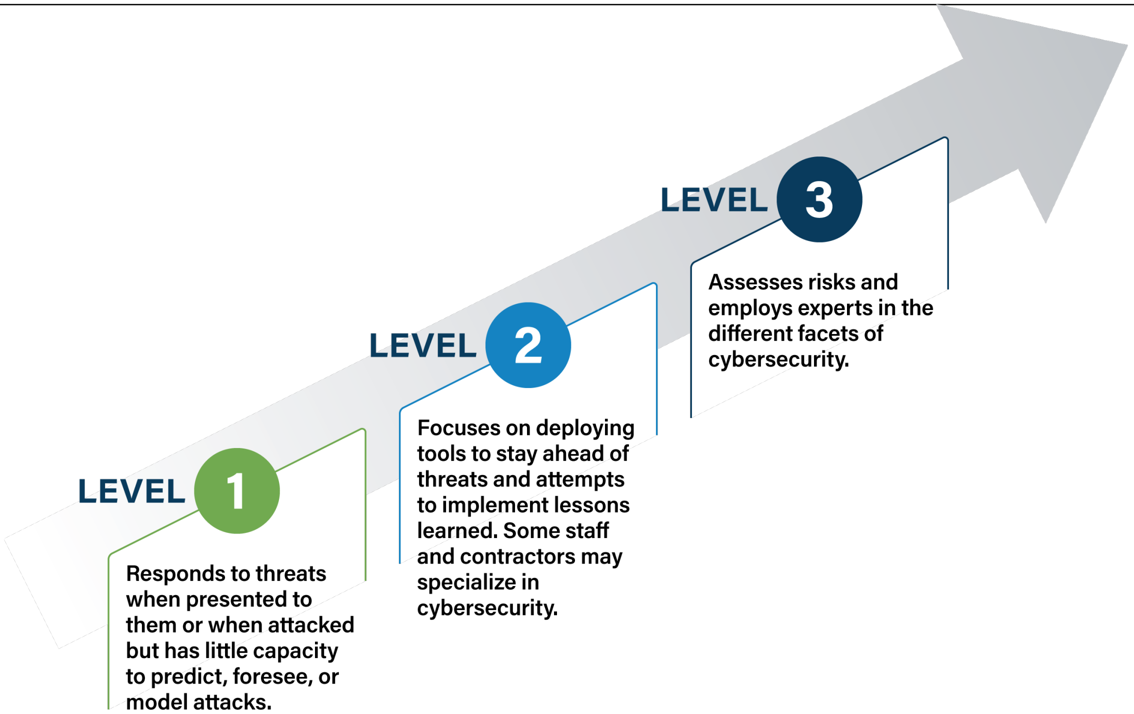
While an election office should implement best practices that best fit its needs, establishing maturities provides rough contours around these differences. By defining maturities, CIS can provide a starting point that any given office can implement or use to tailor its approach.

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* (page 94) 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.


LEVEL 1
Responds to threats when presented to them or when attacked but has little capacity to predict, foresee, or model attacks.
LEVEL 2
Focuses on deploying tools to stay ahead of threats and attempts to implement lessons learned. Some staff and contractors may specialize in cybersecurity.
LEVEL 3
Assesses risks and employs experts in the different facets of cybersecurity.

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. Use the best practices priorities for your maturity level:

- Level 1 *best practice priorities* (page 9).
- Level 2 and Level 3 *best practice priorities* (page 12).

CHAPTER

THREE

DETERMINING YOUR MATURITY LEVEL

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're unsure of what maturity properly represents your jurisdiction, begin at the Level 1 maturity and move upward as appropriate.

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[2] (*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.

Now go implement the Level 1 *best practice priorities* (page 9)!

[2] https://www.cisecurity.org/ms-isac/services/ncsr

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).

Now go implement the Level 2 and Level 3 *best practice priorities* (page 12)!

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.

Now go implement the Level 1 *best practice priorities* (page 9) or the Level 2 and Level 3 *best practice priorities* (page 12)!

CHAPTER FOUR

PRIORITIZING BEST PRACTICES FOR THE LEVEL 1 MATURITY

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. For example, 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.

How do you improve your cybersecurity posture?
Commit!
Complete 1 simple task each week.
Implement 1 best practice each month.
Set aside a minimum amount of resources each quarter.

4.1.1 Level 1 Maturity Baseline Priorities

If you are at the Level 1 maturity, we recommend starting with these to establish a baseline of cyber hygiene. This is the starting point to building yourself up to a *defense-in-depth* (page 102) posture.

Actions

1. Download and complete the *worksheets* (page 119) for the Level 1 maturity baseline. There are ten worksheets, all in one downloadable file.
    - Together, these fulfill **all** of the Level 1 baseline priorities.
    - The left column in the table is the name of a Level 1 maturity worksheet described *here* (page 119). On that page you can download one file with all ten worksheets.
    - The right column gives the relevant best practice actions fulfilled by the worksheet(s).

Worksheet	Actions Fullfilled by the Worksheet
• Hardware Inventory • Software Inventory • Data Inventory • Service Provider Inventory • Account Inventory	Action 1 of *Asset Management* (page 24)
Asset Protection Asset Protection	• All actions of *Encrypt Data at Rest* (page 28) • All actions of *Encrypt Data in Transit* (page 31) • Actions 1 and 2 of *Managing Infrastructure* (page 34)
Account Security	All actions under User Recommendations of *User Management* (page 37)
Backup & Recovery	Action 1 of *Backups* (page 42)
Incident Response	Actions 1 and 4 of *Incident Response* (page 45)
Cyber Education	Actions 2 and 3 of *Building and Managing Staff* (page 48)

While effort for each worksheet can vary greatly depending on the size of your office and number of assets (computers, software, etc.), each *worksheet* (page 119) 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 specific to elections:

1. Join the *MS-ISAC* (page 21).
2. *Protect your website* (page 83) with simple and free tools.
3. Implement an *endpoint protection* (page 68) program through a commercial provider or through the MS-ISAC.
4. Implement the *malicious domain blocking and reporting* (page 71) tool for free through the MS-ISAC.
5. Manage your *removable media* (page 87).

If you complete these, you have implemented all of the priority best practices for the Level 1 maturity! Keep working on other *in scope best practices* (page 16) and work your way up to the Level 2 maturity!

CHAPTER

FIVE

PRIORITIZING BEST PRACTICES FOR THE LEVEL 2 AND LEVEL 3 MATURITIES

5.1 Level 2 and Level 3 Maturities

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

5.1.1 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[3] 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* (page 94). In short, the Community Defense Model is a data-driven, prioritized approach to building yourself up to a *defense-in-depth* (page 102) posture.

Using authoritative data sources like the Verizon Data Breach Investigations Report[4], 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[5] 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.

[3] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

[4] https://www.verizon.com/business/resources/reports/dbir/

[5] http://attack.mitre.org

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.

This efficiency ranking drives the ordering of the best practices in this Guide, with some exceptions particular to elections. While we recommend following the prescribed order, do what's best for your environment and, most importantly, keep making progress!

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* (page 34)
2	4.7	Manage Default Accounts on Enterprise Assets and Software	*Managing Infrastructure* (page 34)
3	5.3	Disable Dormant Accounts	*User Management* (page 38)
4	6.1	Establish an Access Granting Process	*User Management* (page 38)
5	6.2	Establish an Access Revoking Process	*User Management* (page 38)
6	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	*Managing Infrastructure* (page 34)
7	18.3	Remediate Penetration Test Findings	*Remediate Pen Test Findings* (page 56)
8	18.5	Perform Periodic Internal Penetration Tests	*Internal Pen Testing* (page 59)
9	6.8	Define and Maintain Role-Based Access Control	*User Management* (page 38)
10	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	*Managing Infrastructure* (page 34)
11	3.12	Segment Data Processing and Storage Based on Sensitivity	*Network Segmentation* (page 61)
12	5.2	Use Unique Passwords	*User Management* (page 38)
13	6.4	Require MFA for Remote Network Access	*Managing Remote Connections* (page 63)
14	6.5	Require MFA for Administrative Access	*User Management* (page 38)
15	12.8	Maintain Dedicated Computing Resources for All Administrative Work	*Managing Infrastructure* (page 34)
16	2.3	Address Unauthorized Software	*Asset Management* (page 25)
17	2.5	Allowlist Authorized Software	*Asset Management* (page 25)
18	4.2	Maintain a Secure Configuration Process for Network Infrastructure	*Managing Infrastructure* (page 34)
19	4.4	Implement and Manage a Firewall on Servers	*Firewalls and Port Restrictions* (page 66)
20	6.3	Require MFA for Externally-Exposed Applications	*User Management* (page 38)

The best practices in the right column are listed as priority actions in the *best practice index* (page 16) and should be implemented first for the Level 2 and Level 3 maturities.

CHAPTER

SIX

INDEX OF BEST PRACTICES

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

- "Priority" means you should focus on that best practice before other best practices.
- "In Scope" means you should complete that best practice.
- "Out of Scope" means the best practice doesn't apply to you.

For more details on maturities in this Guide, see the *maturities descriptions* (page 4).

To learn how to determine the maturity at which your organization operates, see the *maturity determination* (page 6) guide.

CIS 's Community Defense Model drives the ordering of these best practices. We encourage you to follow this order, but every organization is different, so make adjustments as necessary.

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 prioritized best practices for the Level 1 *maturity* (page 9) and Level 2 and Level 3 *maturities* (page 12).

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

Table 1: Index of Best Practices

✓	#	Best Practice	Maturity Priorities		
			Level 1	Level 2	Level 3
	1	*Addressing Physical Threats* (page 18)	Priority	Priority	Priority
	2	*Join the MS-ISAC* (page 21)	Priority	Priority	Priority
	3	*Asset Management* (page 23)	Priority	Priority	Priority
	4	*Encrypt Data at Rest* (page 27)	Priority	Priority	Priority
	5	*Encrypt Data in Transit* (page 30)	Priority	Priority	Priority
	6	*Managing Infrastructure with Secure Configurations* (page 33)	Priority	Priority	Priority
	7	*User Management* (page 36)	Priority	Priority	Priority
	8	*Backups* (page 41)	Priority	Priority	Priority
	9	*Incident Response Planning* (page 45)	Priority	Priority	Priority
	10	*Building and Managing Staff* (page 48)	Priority	Priority	Priority

continues on next page

Table 1 – continued from previous page

✓	#	Best Practice	Maturity Priorities		
			Level 1	Level 2	Level 3
	11	*Patching and Vulnerability Management* (page 50)	In scope	In scope	In scope
	12	*Remediate Penetration Test Findings* (page 55)	Out of scope	Out of scope	In scope
	13	*Perform Internal Penetration Test* (page 58)	Out of scope	Out of scope	In scope
	14	*Network Segmentation Based on Sensitivity* (page 60)	In scope	Priority	Priority
	15	*Managing Remote Connections* (page 62)	In scope	Priority	Priority
	16	*Firewalls and Port Restrictions* (page 65)	In scope	Priority	Priority
	17	*Endpoint Protection* (page 68)	In scope	In scope	In scope
	18	*Malicious Domain Blocking and Reporting* (page 71)	In scope	In scope	In scope
	19	*Network Monitoring and Intrusion Detection* (page 74)	Out of scope	In scope	In scope
	20	*Managing Wireless Networks* (page 77)	In scope	In scope	In scope
	21	*Public-Facing Network Scanning* (page 80)	In scope	In scope	In scope
	22	*Website Security* (page 83)	In scope	In scope	In scope
	23	*Managing Removable Media* (page 87)	In scope	In scope	In scope
	24	*Exercising Plans* (page 89)	In scope	In scope	In scope
	25	*Formal Cybersecurity Assessments* (page 91)	In scope	In scope	In scope
	26	*Implementing the CIS Controls* (page 94)	In scope	In scope	In scope
	27	*Managing Inaccurate Election Information* (page 97)	In scope	In scope	In scope
	28	*Managing Vendors* (page 100)	In scope	In scope	In scope
	29	*Defense-in-Depth* (page 102)	In scope	In scope	In scope
	30	*Artificial Intelligence in Elections* (page 105)	In scope	In scope	In scope
	30	*Preparing for Election Day Disruptions* (page 108)	In scope	In scope	In scope

CHAPTER

SEVEN

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 and voicemails that criticize their work. However, attempts to threaten or intimidate are unacceptable, and officials should report any such behavior immediately. Doxing is also unacceptable. This is the publishing of an individual's personal information online which can increase the risk of physical threats and intimidation.

There are resources available to help and support you and your team and to give guidance on proactive steps you can take. Several of these are listed below. **If you feel there is any chance of an immediate risk to you or others, do not wait, call 911.**

7.1 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.

7.2 Actions

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

1. 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[6] and ask to speak to the Election Crimes Coordinator.
    - Contact your local CISA Physical Security Advisor[7] (PSA).

[6] https://www.fbi.gov/contact-us/field-offices

[7] https://www.cisa.gov/protective-security-advisors

2. Learn about doxing and take action to minimize risk through CISA's Insight on Mitigating the Impacts of Doxing on Critical Infrastructure[8].

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.

7.3 Cost-Effective Tools

- CISA's Insight on Mitigating the Impacts of Doxing on Critical Infrastructure[9].
- U.S. Election Assistance Commission (EAC): Security Resources for Election Officials[10] and Personal Security for Election Officials[11].
- The Committee for Safe and Secure Elections, CSSE's Five Steps to Safer Elections[12], providing guidance and tabletop exercises to help election administrators and law enforcement work together to strengthen our elections.
- CSSE's Law Enforcement Reference Guides[13], providing state-specific information about laws governing elections.

7.4 Learn More

- CISA's Security Resources[14] for the Election Infrastructure Subsector.
- CISA's De-Escalation Series for Critical Infrastructure[15], offering guidance on how to recognize the warning signs of someone on a path to violence; assess if the situation or person of concern is escalating, or if an emergency response is needed immediately; de-escalate the situation currently taking place; and report the situation.
- Contact elections@cisecurity.org for more information.

[8] https://www.cisa.gov/sites/default/files/publications/CISA%20Insight_Mitigating%20the%20Impacts%20of%20Doxing_508.pdf

[9] https://www.cisa.gov/sites/default/files/publications/CISA%20Insight_Mitigating%20the%20Impacts%20of%20Doxing_508.pdf

[10] https://www.eac.gov/election-officials/election-official-security

[11] https://www.eac.gov/sites/default/files/Personal_Security_for_Election_Officials.pdf

[12] https://safeelections.org/five-steps-to-safer-elections

[13] https://safeelections.org/resources

[14] https://www.cisa.gov/sites/default/files/publications/security_resources_election_subsector_508.pdf

[15] https://www.cisa.gov/de-escalation-series

7.5 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

7.6 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

CHAPTER

EIGHT

JOIN THE MS-ISAC

CIS and the Multi-State ISAC (*MS-ISAC*) are available to provide a wide range of tools, resources, and support for all state, local, tribal, and territorial government organizations, including election offices.

Membership in the MS-ISAC is open to all state, local, tribal, and territorial government organizations in the United States of America. It's a free and voluntary membership for eligible organizations.

The MS-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* (page 71)
- *Endpoint Detection and Response* (page 68)
- Implementing and managing risk to the *CIS Controls* (page 94)
- *Network monitoring* (page 74) via the Albert sensor
- 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

8.1 Goals

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

8.2 Actions

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

1. Join the MS-ISAC. Simply sign up here[16].
    - Contact the MS-ISAC at info@msisac.org with any questions about membership.

8.3 Cost-Effective Tools

- The MS-ISAC has many free tools available to you once you become a member[17].

8.4 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

8.5 Mapping to CIS Handbook Best Practices

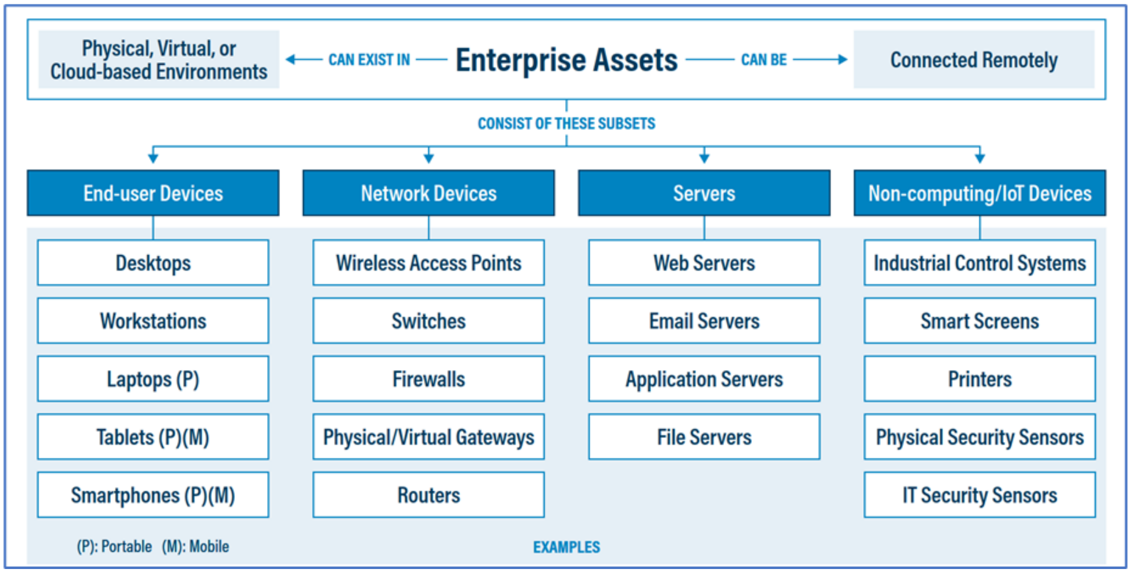
- There are no relevant Handbook best practices.

[16] https://learn.cisecurity.org/ms-isac-registration
[17] https://learn.cisecurity.org/ms-isac-registration

CHAPTER NINE

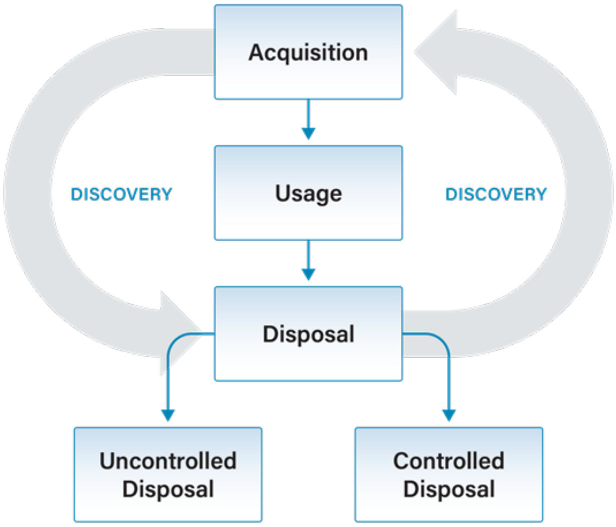
ASSET MANAGEMENT

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. Assets can take many forms, with varying complexity and value to the organizations.



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. All assets have a lifecycle and need that lifecycle managed.

You should also know how to dispose of assets. Various types of hardware and software have specific disposal procedures based on the criticality and sensitivity of the equipment and the data it contains.



9.1 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)
4. Properly dispose of assets (Level 1 maturity)

9.2 Actions

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

9.2.1 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* (page 119) as a template or the CIS Enterprise Asset Inventory Worksheet[18].

- 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.
3. Properly dispose of assets, including shredding paper assets, wiping software assets, and decommissioning hardware assets. Follow all relevant laws for retaining and disposing of all assets.
   - Both NIST[19] and the EAC[20] have extensive guidance on IT asset sanitation and disposal.

9.2.2 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.

[18] https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/
[19] https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
[20] https://www.eac.gov/sites/default/files/Grants/Disposal_Sale_Destruction_Voting-Equipment_V2.pdf

9.3 Cost-Effective Tools

- CIS Enterprise Asset Inventory Worksheet[21]: An excel workbook suitable for small operations with a limited number of assets
- GCA Cybersecurity Toolkit for Elections: Know What You Have[22]: A toolbox with links to free tools relevant to this best practice
- Nmap[23]: Famous multipurpose network scanner used by system administrators and hackers across the world to identify which devices are connected to your network
- ZenMap[24]: Easy-to-use graphic user interface for Nmap
- Spiceworks[25]: Free IT inventory and asset management software to identify devices and software on your network

9.4 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)

9.5 Mapping to CIS Handbook Best Practices

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

[21] https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/
[22] https://gcatoolkit.org/elections/know-what-you-have/
[23] https://nmap.org/
[24] https://nmap.org/zenmap/
[25] https://www.spiceworks.com/

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* (page 119) as a template to track your work.
    - The *cost effective tools* (page 28) section below may help, depending on the types of systems you have in your environment.
2. Encrypt backups. Use the *backups* (page 41) 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[26] provides the U.S. federal requirements for encryption standards to secure data at different sensitivity and classification levels.

NIST Special Publication 800-122[27] provides the U.S. federal requirements for protecting the confidentiality of personal information.

10.3 Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Update Your Defenses[28]: A toolbox with links to free tools relevant to this best practice
- Bitlocker[29]: Built-in encryption for supported Microsoft® Windows devices.
- FileVault[30]: Built-in encryption for MacOS devices.
- Veracrypt[31]: Open-source, free full disk encryption utility.
- EaseUS[32]: This free program can encrypt system images.

[26] https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final
[27] https://csrc.nist.gov/publications/detail/sp/800-122/final
[28] https://gcatoolkit.org/elections/update-your-defenses/
[29] https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx
[30] https://support.apple.com/en-us/HT204837
[31] https://www.veracrypt.fr/en/How%20to%20Back%20Up%20Securely.html
[32] https://www.easeus.com/backup-software/tb-free.html

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

ENCRYPT DATA IN TRANSIT

Any data that is being actively transferred, termed “data in transit,” can present substantial risks for election offices. One of the biggest risks to election integrity occurs when transferring ballot definition files, ballot PDFs, and other such data between otherwise well-protected devices.

For the purposes of this guide, data in transit may refer to data sent over a network. Data stored on physical media being moved from one physical location to another are addressed in the *removable media best practice* (page 87). Data stored on other storage devices, like local storage on a computer or network storage are addressed in the *encrypt data at rest* (page 27).

An election office will often move data between its own systems and between its systems and those of vendors or other partners. An important example is transferring ballot PDFs to a commercial printer that produces the paper ballots for an upcoming eleciton.

The most important thing to know about encrypting data in transit is that the common ways you transfer data are typically easily distinguished between encrypted and unencrypted, or secure and insecure, implementations. These different implementations are called protocols. For instance, you should never transfer, exchange, or submit important data (election data, user credentials, or the like) via a website that starts with HTTP; it should always start with HTTPS.

Encrypted data transfer protocols are ubiquitous; you just need to make sure you and whomever you’re exchanging data with use them.

11.1 Goals

1. Use encrypted protocols when transferring all important data (Level 1 maturity)
2. Ensure vendors and other partners encrypt data in transit (Level 1 maturity)

11.2 Actions

For Encrypt Data in Transit, the necessary actions are the same for all maturity levels.

1. Use encrypted data transfer protocols for all sensitive data.
   - Use HTTPS, not HTTP
   - Use FTPS, SFTP, SCP, or WebDAV over HTTPS, not FTP or RCP
   - Use SSH2, not Telnet
   - Use RDP, not VNC
2. Use an up-to-date version of these protocols compatible with your systems, for instance TLS v1.2 or 1.3, not TLS 1.1 or 1.0.
3. Set defaults for these protocols and versions wherever possible throughout your systems.
4. Impose the same encryption requiremens on vendors and other partners as you use yourselves.
   - You can use the *managing vendors* (page 100) best practices to help implement appropriate best practices across all of your vendors.

11.3 Cost-Effective Tools

- Appropriate encryption capabilities are very likely built into the tools and services you are already using. For most, the proper configuration – turning them on and setting them to use the version you want – is all that is necessary.

11.4 Mapping to CIS Controls and Safeguards

- 3.10: Encrypt Sensitive Data in Transit
- 12.6 Use of Secure Network Management and Communication Protocols
- 15.4: Ensure Service Provider Contracts Include Security Requirements

11.5 Mapping to CIS Handbook Best Practices

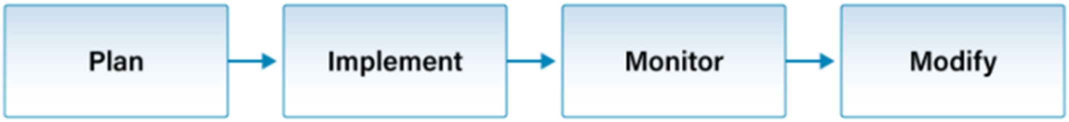
- 8, 12, 84

CHAPTER

TWELVE

MANAGING INFRASTRUCTURE WITH SECURE CONFIGURATIONS

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.

12.1 Goals

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

12.2 Actions

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

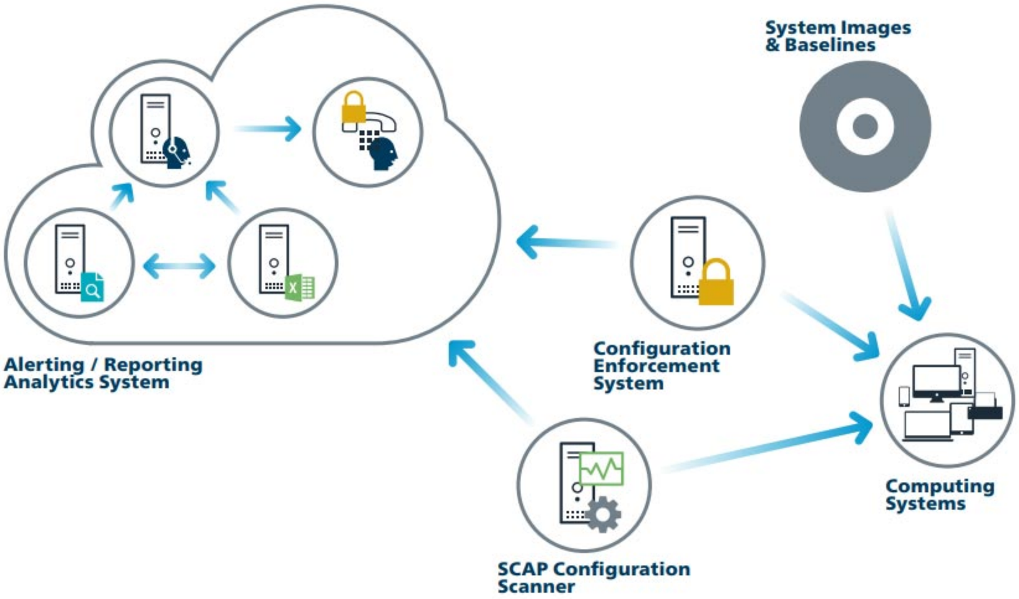
12.2.1 Level 1 Maturity

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* (page 36) 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.

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. Leverage the CIS Benchmark[33] 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[34] for servers, desktops, laptops, mobile devices, and software on systems.
   - Use the *EMS* Gateway Benchmark[35] for machines that, through removable media, exchange data with the EMS.
   - Uninstall or disable unnecessary services on enterprise assets and software


System Images & Baselines
Alerting / Reporting Analytics System
Configuration Enforcement System
Computing Systems
SCAP Configuration Scanner

[33] https://www.cisecurity.org/cis-benchmarks/
[34] https://www.cisecurity.org/cis-benchmarks/
[35] https://www.cisecurity.org/insights/blog/new-guidance-to-secure-election-management-system-machines

12.3 Cost-Effective Tools

- Applocker[36]: Free Microsoft® Windows tool to identify and restrict the software that is allowed to run.
- Netwrix[37]: Variety of free tools to identify information about administrative access on your systems.
- OpenAudIT[38]: Inventory applications and software on workstation servers and network devices.
- CIS Benchmarks[39]: Secure configurations for more than a hundred of the most common software applications.
- Election Management System Gateway Benchmark[40]: A CIS Benchmark to secure the machines that, through removable media, exchange data with the EMS.

12.4 Mapping to CIS Controls and Safeguards

- 4.1: Establish and Maintain a Secure Configuration Process (Level 1 maturity)
- 4.2: Establish a Secure Configuration Process for Network Infrastructure (Level 1 maturity)
- 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)

12.5 Mapping to CIS Handbook Best Practices

- 23, 27, 65, 68, 88

[36] https://technet.microsoft.com/en-us/library/dd759117(v=ws.11).aspx
[37] https://www.netwrix.com
[38] http://www.open-audit.org/
[39] https://www.cisecurity.org/cis-benchmarks/
[40] https://www.cisecurity.org/insights/blog/new-guidance-to-secure-election-management-system-machines

CHAPTER

THIRTEEN

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.

13.1 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)

13.2 Actions

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

13.2.1 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 create passwords or security questions using 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. 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.
5. 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 *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.
   - Realistically, some devices or applications may require shared accounts. These accounts should receive formal exceptions from management and their usage appropriately tracked.
   - When this is the case, 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. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.
9. 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.
10. Allow and encourage use of password managers.

13.2.2 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 *MS-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.

13.3 Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Beyond Simple Passwords[41]: A toolbox with links to free tools relevant to this best practice.
- have i been pwned password breach service[42]: A site for searching for breached accounts. Includes and API to automate searching for breached accounts.

[41] https://gcatoolkit.org/elections/beyond-simple-passwords/

[42] https://haveibeenpwned.com

13.4 Learn More

- Get more password guidance from *NIST*: SP 800-63B Section 5.1.1.2[43].
- Password spotlight[44] (This spotlight has some out-of-date recommendations. Use in conjunction with the NIST guidance).
- Understand the logic behind using passphrases[45].

13.5 Mapping to CIS Controls and Safeguards

- 3.3 Configure Data Access Control Lists (Level 1 maturity)
- 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)
- 3.14 Log Sensitive Data Access (Level 3 maturity)

[43] https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver
[44] https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-passwords
[45] https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

13.6 Mapping to CIS Handbook Best Practices

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

CHAPTER

FOURTEEN

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.

14.1 Goals

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

14.2 Actions

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

14.2.1 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.

14.2.2 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.

14.3 Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Backup and Recover[46]: A toolbox with links to free tools relevant to this best practice.
- Microsoft® Volume Shadow Copy Service[47] (VSS): Tool to create backup copies or snapshots of files or volumes.
- VeraCrypt[48]: Free, open source, on-the-fly encryption.
- Clonezilla®[49]: Partition, disk imaging, and cloning tool.
- Apple Time Machine[50]: 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[51]: 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[52]: 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[53]: In Windows 11, you can restore files from a backup created with Backup and Restore or File History.
- No More Ransom[54]: Website to help victims of ransomware retrieve their data, report a crime, and more.

[46] https://gcatoolkit.org/elections/backup-and-recover/
[47] https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service
[48] https://veracrypt.fr/en/Home.html
[49] https://clonezilla.org
[50] https://support.apple.com/en-us/HT201250
[51] http://www.amanda.org
[52] https://www.bacula.org
[53] https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c
[54] https://www.nomoreransom.org

14.4 Learn More

- DHS, CISA, and MS-ISAC Joint Ransomware Guide[55]: A guide written by US federal agencies to assist with ransomware.

14.5 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)

14.6 Mapping to CIS Handbook Best Practices

- 21, 60

[55] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

CHAPTER

FIFTEEN

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.

15.1 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)

15.2 Actions

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

15.2.1 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[56] for disaster planning.
        - CISA's Incident Response Support for Election Partners[57].

[56] https://www.eac.gov/documents/2017/08/03/six-tips-contingency-and-disaster-planning-eac
[57] https://www.cisa.gov/sites/default/files/publications/incident_handling_elections_final_508_0.pdf

   - The Belfer Center's Election Playbook[58].

2. *Exercise your plan* (page 89) regularly. At least once a year; before each election is better.
3. When an incident does occur, execute your plan.
   - The MS-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

15.2.2 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.

15.3 Cost-Effective Tools

- CIS's Cyber Incident Checklist[59]: Helps organizations deal with a cyber incident by 1) establishing reliable facts and a way to stay informed, 2) mobilizing a response, and 3) communicating what you know

15.4 Learn More

- CISA's Incident and Vulnerability Response Playbooks[60]: Although intended for federal agencies, election offices should review them to benchmark their own vulnerability and incident response practices.
- The incident reponse sections of the Belfer Center's Elections Battle Staff Playbook[61]: Guidance to help you develop incident trackers, train staff, and test your processes.

15.5 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)

[58] https://www.belfercenter.org/publication/elections-battle-staff-playbook

[59] https://www.cisecurity.org/insights/white-papers/cyber-incident-checklist

[60] https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

[61] https://www.belfercenter.org/publication/elections-battle-staff-playbook

- 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)

15.6 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

CHAPTER

SIXTEEN

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.

16.1 Goals

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

16.2 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* (page 119) as a template.
4. Implement actions for proper logical access in *User Management* (page 36)
5. Implement actions for proper system configuration in *Managing Infrastructure* (page 33)

16.3 Learn More

- MS-ISAC® Cybersecurity Awareness Toolkit[62] features educational materials designed to raise cybersecurity awareness. Digital materials are aggregated for your use.
- Federal Virtual Training Environment[63] (FedVTE): Online Courses Free online cybersecurity training to State, Local, Tribal, and Territorial (SLTT) governments.
- Learn how to protect yourself, your family and your devices with tips and resources from the National Cybersecurity Alliance's Stay Safe Online[64] initiative. See also its YouTube channel[65].

16.4 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)

16.5 Mapping to CIS Handbook Best Practices

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

[62] https://www.cisecurity.org/ms-isac/ms-isac-toolkit
[63] https://fedvte.usalearning.gov
[64] https://staysafeonline.org/stay-safe-online
[65] https://www.youtube.com/user/StaySafeOnline1

CHAPTER

SEVENTEEN

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 *MS-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[66] (*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[67] 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.

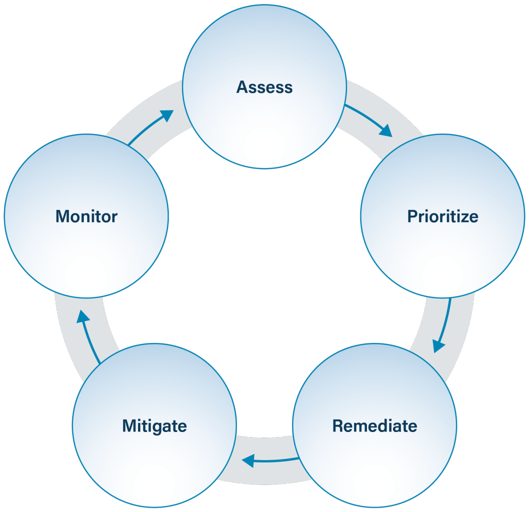
The *MS-ISAC* regularly disseminates Cybersecurity Advisories[68], which address critical patches in commercial software commonly used by government agencies. To subscribe to Cybersecurity Advisories, *MS-ISAC* members should contact their account manager or complete the subscription form[69].

[66] https://nvd.nist.gov

[67] https://nvd.nist.gov/general/FAQ-Sections/General-FAQs

[68] https://www.cisecurity.org/resources/advisory/

[69] https://learn.cisecurity.org/ms-isac-subscription



17.1 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)

17.2 Actions

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

17.2.1 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.

17.2.2 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* (page 23). 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[70].

[70] https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2017/03/Patching-TLP-WHITE.pdf

17.3 Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Update Your Defenses[71]: A toolbox with links to free tools relevant to this best practice.
- GCA Cybersecurity Toolkit for Elections: Control Access[72]: A toolbox with several links to free tools relevant to this best practice.
- CIS Benchmarks™[73]: Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices.
- CIS SecureSuite® Membership[74]: No-cost membership to MS-ISAC members, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more.
- CIS-CAT® Pro Tool[75]: Scans for proper CIS Benchmark configurations for applications, operating systems, and network devices.
- Itarian[76]: Patch management solution for Windows.
- Opsi[77]: A more complicated solution that can help to manage both Windows and Linux platforms.
- OpenVAS[78]: Free, open-source framework for vulnerability scanning and management.
- Nmap[79]: Famous multipurpose network scanner used by system administrators and hackers across the world to identify which devices are connected to your network.
- U.S. National Vulnerability Database[80] (NVD): Repository of standards based on vulnerability management data.

17.4 Learn More

- The MS-ISAC's Technical White Paper Timely Patching Reduces System Compromises[81]
- Apple Auto-update - iOS[82]
- Apple Auto-update - MacOS[83]

[71] https://gcatoolkit.org/elections/update-your-defenses/
[72] https://gcatoolkit.org/elections/control-access/
[73] https://www.cisecurity.org/benchmark
[74] https://www.cisecurity.org/cis-securesuite
[75] https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro
[76] https://www.itarian.com
[77] https://www.opsi.org
[78] https://www.openvas.org
[79] https://nmap.org/
[80] https://nvd.nist.gov
[81] https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2017/03/Patching-TLP-WHITE.pdf
[82] https://support.apple.com/en-us/HT202180
[83] https://support.apple.com/en-us/HT201541

- Auto-update Windows[84]
- Auto-update MS Office on macOS[85]
- Auto-update Android[86]

17.5 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

17.6 Mapping to CIS Handbook Best Practices

- 43, 44, 76

[84] https://support.microsoft.com/en-us/windows/keep-your-pc-up-to-date-de79813c-7919-5fed-080f-0871c7bd9bde

[85] https://support.microsoft.com/en-us/office/update-office-for-mac-automatically-bfd1e497-c24d-4754-92ab-910a4074d7c1?ui=en-us&rs=en-us&ad=us

[86] https://support.google.com/googleplay/answer/113412

CHAPTER

EIGHTEEN

REMEDIATE PENETRATION TEST FINDINGS

Often, penetration tests are performed for specific purposes:

- As a “dramatic” demonstration of an attack, usually to convince decision-makers of their enterprise’s weaknesses
- As a means to test the correct operation of enterprise defenses (“verification”)
- To test that the enterprise has built the right defenses in the first place (“validation”)

This best practice looks to address what occurs once the penetration testing has been completed. The organization performing the penetration test will provide a written report of their results. It is becoming increasingly popular to conduct penetration tests through third-party legal counsel to protect the penetration test report from disclosure. Once a report is received, the security team and other affected parties within the organization should review the report to understand the findings. The organization performing the test is often available for questions to clarify issues documented in the report.

Issues within the report should then be priortized. As a simple method, some organizations may choose to use the Common Vulnerability Scoring System[87] (term:*CVSS*) which can provide a severity rating for vulnerabilities. But CVSS severity ratings shoudln’t leveraged blindly; a 5/10 in a production system handling election data that is exposed to the internet is likely more important than a 7/10 in an internal testing system that lacks sesntive data.

Specific individuals working to fix issues from the report should report back that the fixes have been successfully completed so that they can be validated by the appropriate internal team.

18.1 Goals

1. Work to understand the results report from the penetration test. Create a plan to remediate findings in a logical manner, according to the severity of the findings (Level 3 maturity)

[87] https://nvd.nist.gov/vuln-metrics/cvss

18.2 Actions

18.2.1 Level 1 and Level 2 Maturities

There are no actions for Level 1 and Level 2.

18.2.2 Level 3 Maturity

1. Review and understand the results of the penetration testing report with all IT and security staff that have responsibilities.
2. Ask questions of the organization that performed the penetration test to clarify any misunderstandings or concerns that may require an update to the report.
3. Create a list of items to fix.
4. Prioritize this list based on severity.
5. Assign list items to appropriate personnel.

18.3 Cost-Effective Tools

- OWASP Penetration Testing Methodologies[88]: This link contains a collection of penetration testing methodologies.

18.4 Learn More

- PCI Security Standards Council[89]: A set of standards used by the Payment Card Industry (PCI) for perfomring penetration testieng. Includes qualifications for testers and a technical methodology.

18.5 Mapping to CIS Controls and Safeguards

- 18.3: Remediate Penetration Test Findings
- 18.4: Validate Security Measures

[88] https://www.owasp.org/index.php/Penetration_testing_methodologies

[89] https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

18.6 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

CHAPTER

NINETEEN

PERFORM INTERNAL PENETRATION TEST

Internal penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration tests are expensive, complex, and potentially introduce their own risks. Experienced individuals from reputable organizations must conduct them. Accordingly, it is rare that this expertise already exists within an election office. Some risks include unexpected shutdown of systems that might be unstable, exploits that might delete or corrupt data or configurations, and the output of a testing report that needs to be protected itself, because it gives step-by-step instructions on how to break into the enterprise to target critical assets or data.

19.1 Goals

1. Conduct a penetration test of internal jurisdiction assets with capable and trustworthy organizations (Level 3 maturity)
2. Understand and correct findings of the results report in a timely manner (Level 3 maturity)

19.2 Actions

19.2.1 Level 1 and Level 2 Maturities

There are no actions for Level 1 and Level 2.

19.2.2 Level 3 Maturity

1. Identify high and low-value election assets requiring internal penetration testing.
2. Identify a suitable organization for performing the testing. These resources may be available via a state agency, university, or third-party company. Note that it is rare that this expertise already exists within an election organization.

19.3 Cost-Effective Tools

- OWASP Penetration Testing Methodologies[90]: A collection of penetration testing methodologies.

19.4 Learn More

- PCI Security Standards Council[91]: A set of standards used by the Payment Card Industry (PCI) for perfomring penetration testieng. Includes qualifications for testers and a technical methodology.

19.5 Mapping to CIS Controls and Safeguards

- 18.1: Establish and Maintain a Penetration Testing Program
- 18.4: Validate Security Measures
- 18.5: Perform Periodic Internal Penetration Tests

19.6 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

[90] https://www.owasp.org/index.php/Penetration_testing_methodologies
[91] https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

CHAPTER TWENTY

NETWORK SEGMENTATION BASED ON SENSITIVITY

Network Segmentation is the practice of splitting a network into multiple sub-networks. These networks are usually designed around business needs, for example, having sub-networks for executives, finance, operations, and human resources or by keeping election functions separated from other county functions. Networks can also be separated by data sensitivity, keeping more sensitive election data separated from every day communications.

Keeping information segmented can shrink the attack surface: successful attacks on one part of a network are less likely to impact the other parts. It can also lead to performance improvements within each sub-network. Users are often required to re-authenticate in order to access other, particularly more sensitive, areas of the network. This can limit how much damage a threat actor can do if they gain access to any given part of a network.

Network segmentation can be physical or logical. Physical segmentation keeps network traffic separate through devices such as firewalls and switches. Logical segmentation uses virtual networks and addressing schemes to keep traffic on its intended sub-network. Additional segmentation can be achieved through network isolation, where an entirely separate network is created. This is often performed in the field of elections for sensitive election data like tabulators. There are often other portions of the election management system that may be connected to an isolated network.

Additionally, organizations may wish to segregate high-risk applications from the general network. For instance, multiple employees may need to access applications used to design ballots, and they all may need to push and pull data from the same election datastore (e.g., fileserver).

Organizations should leverage their data inventories to understand what systems have the most sensitive data. High-risk data, and assets hosting or processing high-risk data, are likely candidates for some form of network segmentation.

20.1 Goals

1. Know whether your election environment needs to segmented and understand the best ways to do so (Level 1 maturity)
2. Deploy appropriate network segmentation tools (Level 1 maturity)
3. Manage network segmentation appropriately (Level 1 maturity)

20.2 Actions

For Network Segmentation Based on Sensitivity, the necessary actions are the same for all maturity levels.

1. Take simple steps to segment traffic, like creating a guest wireless network and a voice network.
2. Leverage the data inventory for identifying high risk assets that should be segmented.
3. Determine your network segmentation strategy, including whether to employ physical segmentation, logical, or both.
4. Deploy a network segmentation tools appropriate for your environment, including establishing policies for firewalls and related devices.
5. Monitor and adjust policies to meet the changing needs of your organization.

20.3 Cost-Effective Tools

- Many states and localities deploy governance, risk, and compliance (*GRC*) tools to help manage security on their networks. Find out what tools you are currently using and whether they have network segmentation capabilties.
- Exising firewalls, switches, and their associated software can also be used to improve network segmentation.

20.4 Mapping to CIS Controls and Safeguards

- 3.12: Segment Data Processing and Storage Based on Sensitivity
- 12.2: Establish and Maintain a Secure Network Architecture
- 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work
- 13.4: Perform Traffic Filtering Between Network Segments

20.5 Mapping to CIS Handbook Best Practices

- 6

CHAPTER

TWENTYONE

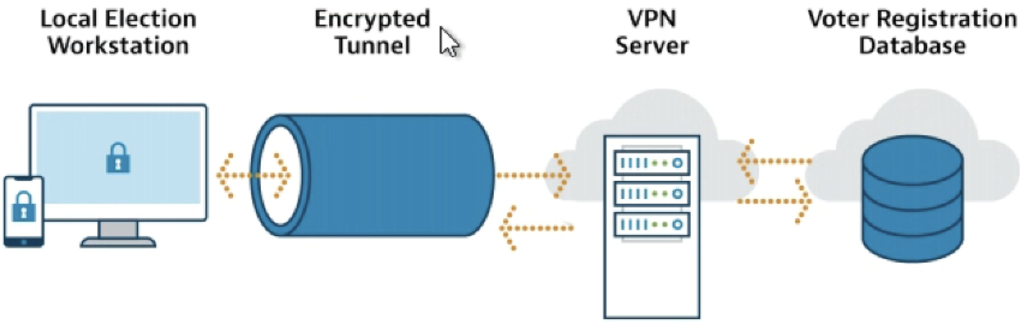
MANAGING REMOTE CONNECTIONS

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[92] 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[93] and here[94], that led to this[95] joint advisory.
2. Review CISA's Enterprise VPN Security Alert[96]
3. Review NIST's Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security[97]

[92] https://www.cisecurity.org/insights/white-papers/cis-controls-telework-and-small-office-network-security-guide
[93] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379
[94] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510
[95] https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2573391/russian-foreign-intelligence-service-exploiting-five-publicl
[96] https://www.cisa.gov/uscert/ncas/alerts/aa20-073a
[97] https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

21.3 Cost-Effective Tools

- CIS's Telework and Small Office Network Security Guide[98]: Assists 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.

21.4 Learn More

- For more tips on working with vendors, review CIS's "A Guide for Ensuring Security in Election Technology Procurements."[99]

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

[98] https://www.cisecurity.org/insights/white-papers/cis-controls-telework-and-small-office-network-security-guide
[99] https://www.cisecurity.org/elections

CHAPTER

TWENTYTWO

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.

22.1 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)

22.2 Actions

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

22.2.1 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.

22.2.2 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[100] for firewall management that is appropriate for your environment.

22.3 Cost-Effective Tools

- Free vulnerability scanning from CISA. Contact vulnerability_info@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services."
- CIS Benchmark[101] for firewall management: Secure configurations for more than a hundred of the most common software applications.

22.4 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)

[100] https://www.cisecurity.org/cis-benchmarks/
[101] https://www.cisecurity.org/cis-benchmarks/

22.5 Mapping to CIS Handbook Best Practices

- 41, 42

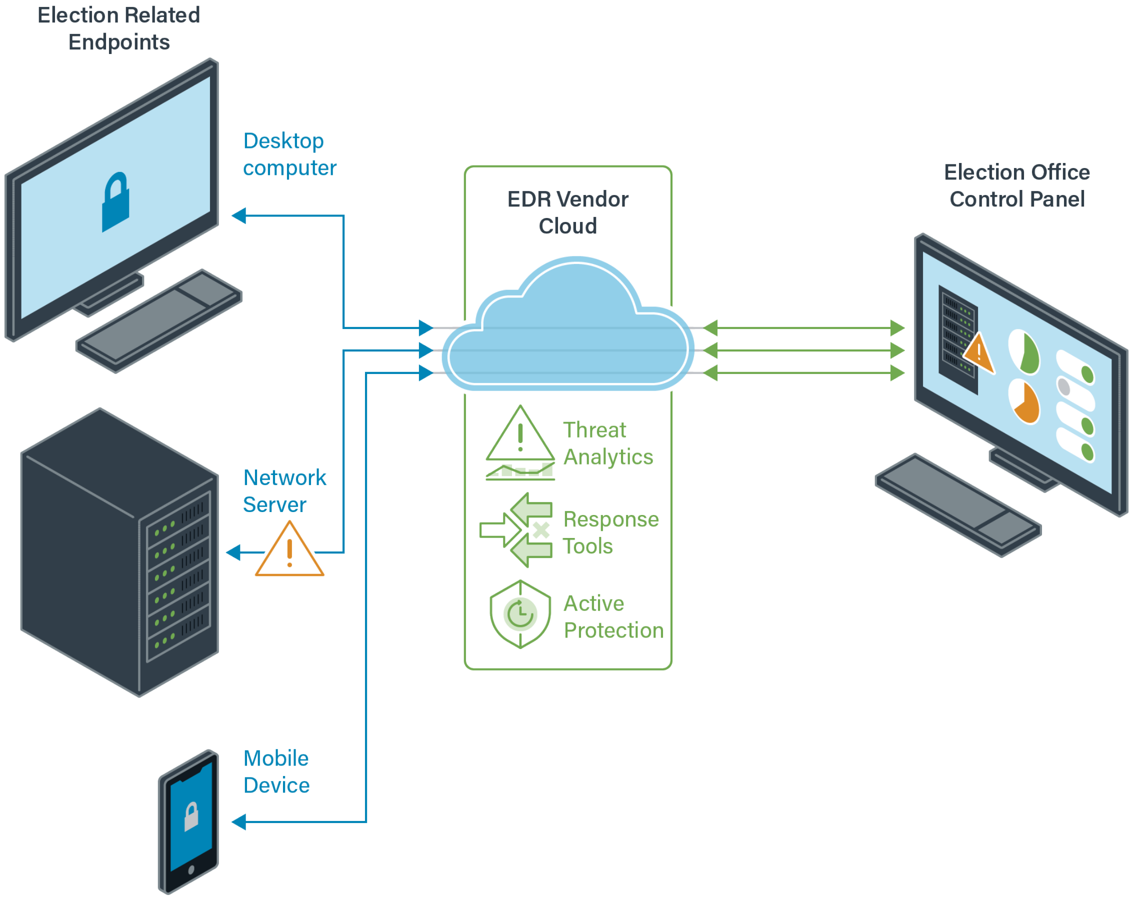
CHAPTER

TWENTYTHREE

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.



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.

23.1 Goals

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

23.2 Actions

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

23.2.1 Level 1 Maturity

1. Deploy EDR on systems throughout your network. EDR should not be deployed on voting systems.
   - You may qualify for federally-funded or discounted EDR through the MS-ISAC. Contact info@msisac.org for more information.
   - For commercial solutions, you may also review CIS's Guide for Ensuring Security in Election Technology Procurements[102] 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 MS-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.

[102] https://www.cisecurity.org/elections

- 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 CIS Cyber Incident Checklist[103] to manage security events.

23.2.2 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 MS-ISAC. Contact info@msisac.org for more information.

23.3 Cost-Effective Tools

- MS-ISAC EDR program: EDR services at no charge or discounted to state and local election offices. Contact info@msisac.org.

23.4 Mapping to CIS Controls and Safeguards

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

23.5 Mapping to CIS Handbook Best Practices

- 32, 40

[103] https://www.cisecurity.org/insights/white-papers/cyber-incident-checklist

CHAPTER

TWENTYFOUR

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.

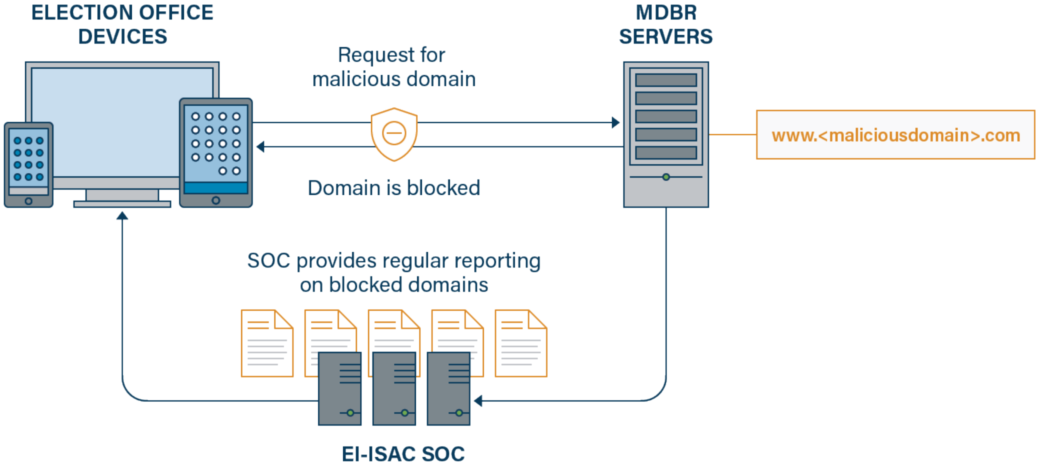

ELECTION OFFICE DEVICES
MDBR SERVERS
Request for malicious domain
Domain is blocked
www.<maliciousdomain>.com
SOC provides regular reporting on blocked domains
EI-ISAC SOC

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

24.1 Goals

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

24.2 Actions

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

1. If you're an MS-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 member, *join today* (page 21) – then complete action #1 of this best practice.

The MS-ISAC provides members with a free MDBR service. Members sign up and configure their DNS server, and the MS-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 MS-ISAC and its provider fully maintain the systems required to provide the service.

The MS-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 MS-ISAC will provide regular reporting and intelligence services for SLTT members.

24.3 Cost-Effective Tools

- MS-ISAC MDBR service[104]: A no-cost, lightweight MDBR solution for MS-ISAC members.

24.4 Mapping to CIS Controls and Safeguards

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

[104] https://mdbr.cisecurity.org

24.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

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 *MS-ISAC* (page 21) 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 MS-ISAC receives any alerts, analyzes them, and works with your office to take any recommended action. The MS-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* (page 9) 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 Cost-Effective Tools

- Zabbix[105]: Monitoring tool for IT infrastructure
- Quad9®[106]: Domain Name System (DNS) filtering service
- OpenDNS®[107]: Domain Name System (DNS) filtering service
- Snort[108]: Open source IDS/IPS maintained by Cisco
- Suricata[109]: Open source intrusion detection system
- Zeek NIDS[110]: Open source network analysis tool with an IDS
- Security Onion[111]: Linux distribution dedicated to network security monitoring

[105] https://www.zabbix.com
[106] https://www.quad9.net
[107] https://www.opendns.com
[108] https://www.snort.org
[109] https://suricata-ids.org
[110] https://www.zeek.org
[111] https://www.securityonion.org

- Skybox Network Assurance[112]: Network security posture management

25.4 Learn More

- NIST Special Publication 800-94[113]: Guide to Intrusion Detection and Prevention Systems (IDPS)

25.5 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

25.6 Mapping to CIS Handbook Best Practices

- 7

[112] https://www.skyboxsecurity.com/products/skybox-network-assurance
[113] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

CHAPTER

TWENTYSIX

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.

26.1 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)

26.2 Actions

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

26.2.1 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* (page 50) 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.

26.2.2 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.

26.2.3 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.

26.3 Cost-Effective Tools

- Aircrack-ng[114]: Wireless security suite
- Kismet[115]: Wireless security and investigation
- Wireshark[116]: Packet capture analysis

[114] https://www.aircrack-ng.org
[115] https://www.kismetwireless.net
[116] https://www.Wireshark.org

26.4 Learn More

- CIS's Mobile Security Companion Guide[117]
- NIST Special Publication 800-153[118]: Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST Special Publication 800-94[119]: Guide to Intrusion Detection and Prevention Systems (IDPS)

26.5 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)

26.6 Mapping to CIS Handbook Best Practices

- 5, 56

[117] https://www.cisecurity.org/blog/new-release-cis-controls-mobile-companion-guide
[118] https://csrc.nist.gov/publications/detail/sp/800-153/final
[119] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

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. Contact the MS-ISAC for information on the 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[120]: 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![121]: 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.

[120] https://www.cisa.gov/cyber-hygiene-services
[121] https://www.grc.com/shieldsup

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

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.

28.1 Introduction

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

28.1.1 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.

28.1.2 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.

28.1.3 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.

28.1.4 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.

28.1.5 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 inaccurate information, including the alteration of time and dates for open voting events or unofficial results. These changes may be subtle and thus difficult to detect.

28.2 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)

28.3 Actions

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

28.3.1 Level 1 Maturity

1. Visit https://get.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[122] and Google[123], will mitigate instances of these attacks.
   - Learn more through the CIS's Guide to DDoS Attacks[124].
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* (page 41) established that can be quickly deployed in place of a compromised website.
   - Maintain *up-to-date software and patch vulnerabilities* (page 50).

28.3.2 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.

[122] https://www.cloudflare.com/athenian/
[123] https://projectshield.withgoogle.com/landing
[124] https://www.cisecurity.org/insights/white-papers/technical-white-paper-guide-to-ddos-attacks

- 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.

28.4 Cost-Effective Tools

- get.gov[125]: The government portal to obtain and manage a .gov domain.
- CyHy program[126]: CISA's cyber hygiene web application scanning program.
- Cloudflare[127]'s Athenian Project: Free security and performance for state and local election websites.
- Google[128]'s Project Shield: A free service that defends news, human rights and election monitoring sites from DDoS attacks.

28.5 Learn More

- Election Security Spotlight – Typosquatting[129]
- The distributed denial-of-service (DDOS) attack section of CISA's Cybersecurity Toolkit to Protect Elections[130].
- CISA's DDOS Quick Guide[131].

28.6 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls

28.7 Mapping to CIS Handbook Best Practices

- 9

[125] https://get.gov
[126] https://www.cisa.gov/cyber-hygiene-web-application-scanning
[127] https://www.cloudflare.com/athenian/
[128] https://projectshield.withgoogle.com/landing
[129] https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-typosquatting
[130] https://www.cisa.gov/cybersecurity-toolkit-protect-elections
[131] https://www.cisa.gov/uscert/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

CHAPTER

TWENTYNINE

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.

29.1 Goals

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

29.2 Actions

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

29.2.1 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[132] 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.

29.2.2 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[133] is the gold standard for such a program.

29.3 Cost-Effective Tools

- CIS's cybermarket[134]: A buying guide for MS-ISAC members, providing products from trusted vendors at discounted rates.

29.4 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)

29.5 Mapping to CIS Handbook Best Practices

- 4, 22, 55, 63

[132] https://www.cisecurity.org/services/cis-cybermarket
[133] https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
[134] https://www.cisecurity.org/services/cis-cybermarket

CHAPTER

THIRTY

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, inaccurate information, power outages, and many other types of incidents.

Generally, you can either take part in exercises offered by others 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.

30.1 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)

30.2 Actions

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

30.2.1 Level 1 Maturity

1. Participate in tabletop exercises 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.

30.2.2 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[135].
2. Have a regular schedule for exercises. Stick to it.

30.3 Cost-Effective Tools

- CISA's critical infrastructure exercise resources[136]: Downloadable exercise planning and comprehensive exercise packages.
- MS-ISAC's tabletop exercise resources[137]: SLTT focused tips, tricks, reviews, and exercise packages for download.

30.4 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

30.5 Mapping to CIS Handbook Best Practices

- 33, 72

[135] https://www.cisa.gov/critical-infrastructure-exercises
[136] https://www.cisa.gov/critical-infrastructure-exercises
[137] https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx

CHAPTER

THIRTYONE

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.

31.1 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)

31.2 Actions

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

31.2.1 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[138] 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.

31.2.2 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[139] 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[140].
   - Tools available to election offices include CIS-CAT[141], which can automate much of the process of implementing appropriate safeguards.

[138] https://www.cisa.gov/cyber-hygiene-services
[139] https://www.cisa.gov/cyber-resource-hub
[140] https://www.cisecurity.org/cis-benchmarks/
[141] https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls

31.2.3 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.

31.3 Cost-Effective Tools

- CISA's Cyber Hygiene Services[142]: 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.
- CIS Controls: see the *CIS Controls* (page 94) best practice
- CIS Benchmarks[143]: Secure configurations for more than a hundred of the most common software applications.
- CIS-CAT Pro[144]: a tool freely available to *MS-ISAC members* (page 21) to support implementation of the CIS Controls

31.4 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.

31.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

[142] https://www.cisa.gov/cyber-hygiene-services
[143] https://www.cisecurity.org/cis-benchmarks/
[144] https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro

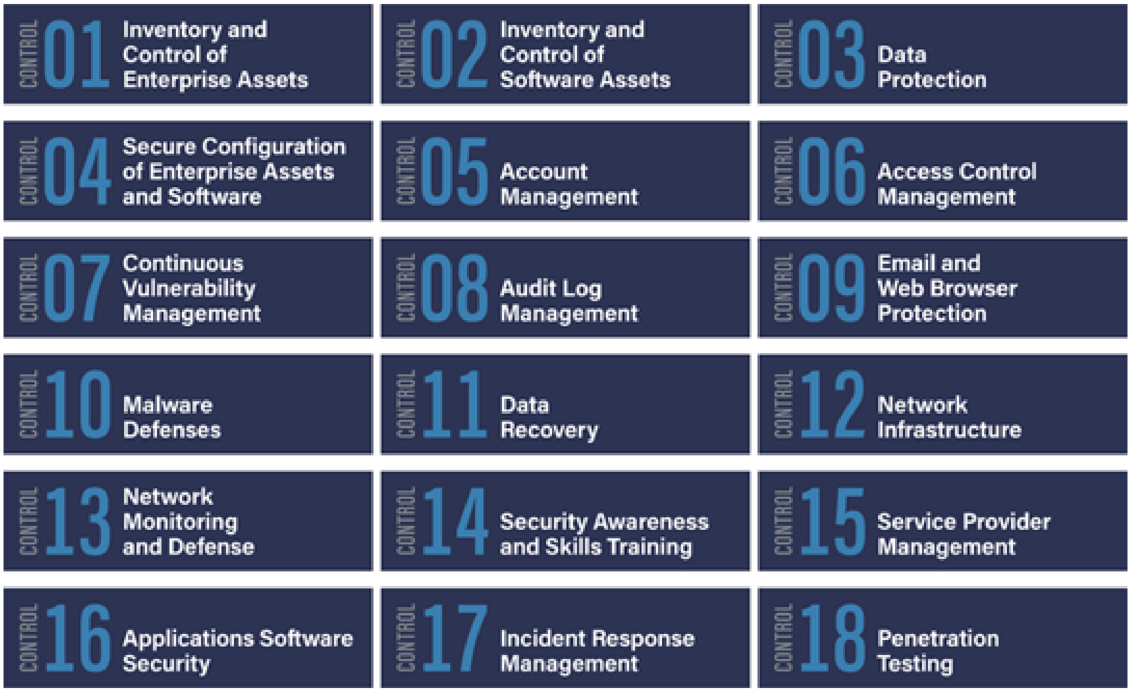
CHAPTER

THIRTYTWO

IMPLEMENTING THE CIS CONTROLS

The CIS Critical Security Controls™[145] 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.



CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

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.

[145] https://www.cisecurity.org/controls

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.

32.1 Goals

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

32.2 Actions

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

32.2.1 Level 1 Maturity

1. Implement the IG1 controls.
   - The easiest way to do this is through the Level 1 *Priorities* (page 9). This will help you complete all of the actions for the Level 1 maturity, including IG1.
   - You can also use the CIS Controls Navigator[146] to get to export a convenient list of the IG1 controls.

[146] https://www.cisecurity.org/controls/cis-controls-navigator

32.2.2 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[147] to get this done.

32.2.3 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[148] to get this done.

32.3 Cost-Effective Tools

- CIS Controls Navigator[149]: A simple tool to allow export of customized sets of safeguards from the CIS Controls.
- CIS Controls version 8[150]: 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.

32.4 Mapping to CIS Controls and Safeguards

- All!

32.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

[147] https://www.cisecurity.org/controls/cis-controls-navigator
[148] https://www.cisecurity.org/controls/cis-controls-navigator
[149] https://www.cisecurity.org/controls/cis-controls-navigator
[150] https://www.cisecurity.org/controls/v8

CHAPTER

THIRTYTHREE

MANAGING INACCURATE ELECTION INFORMATION

Inaccurate information about election administration and its processes is nothing new. Election officials have long worked to ensure voters know their rights and responsibilities–and don't get misled by intentional or unintentional inaccuracies.

Both independent threat actors and large nation-states are capable of manufacturing inaccuracies about elections, and some unintentional mistakes will always happen. Threat actors may have hundreds of people on payroll, choose to conduct operations via automated bots, or both. When users encounter inaccurate information they may be unable to differentiate it from genuine information, sharing it and unwittingly influencing an even wider audience.

Increasingly, these threat actors use artificial intellience in their work. Certainly not all uses of artificial intelligence are nefarious, but it is a tool that can be employed to accelerate the pace of harmful activities and create more believable material. This guide also provides guidance on how to *manage AI in elections* (page 105).

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. 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 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 to ensure the public has the most accurate, timely information about elections. That is the focus of this best practice.

33.1 Goals

1. Recognize how inaccurate information can impact election administration (Level 1 maturity)
2. Take action when you encounter inaccurate information (Level 1 maturity)

33.2 Actions

For Managing Inaccurate Election Information, the necessary actions are the same for all maturity levels.

33.2.1 Preparing for Inaccurate Information

1. Set up *multi-factor authentication* to protect social media accounts from compromise.
2. Establish your office and its communication channels as the authority for information about your jurisdiction.
3. Use a wide variety of public forums to share accurate information about your elections.
4. Regularly publish official messaging about the state of your election infrastructure.
5. Work with local media to promote official sources of information.

33.2.2 Remediating Inaccuracies

1. Establish your office and its communication channels as the authority for information about your jurisdiction by:
   - Communicating with your constituents early and often, and making sure they know the official way to get more information from you.
   - Securing your systems, including *websites* (page 83) and social media accounts, to prevent things like deep fakes being posted on an official channel.
   - Signing up for a *.gov website domain* (page 85) to signal your status as an official government organization
2. Respond to inaccurate information with accurate information as quickly as possible. This rapid response is even more important as an election nears. These activities are sometimes called debunking or pre-bunking, but what's important is that you are getting an accurate message out in a way that helps your voters and the public.
3. Track important information by, for instance, following your county name and the names of your election official and other public figures in social media and new reports.
4. Understand the increasing role of generative artificial intelligence in elections and *what you can do about it* (page 105).

33.3 Cost-Effective Tools

- The Election Assistance Commission's (EAC) Communications 101 Toolkit[151]: A booklet to help election offices successfully communicate with the public, and plan for challenges that may arise throughout their work.
- The EAC's Election Official Social Media Toolkit[152]: A centralized resource to streamline social media efforts, ensuring consistent and impactful communication.
- The EAC's Communications for Election Officials 101 YouTube video series[153]: Short, practical resources on topics like writing key messages, identifying spokespeople, and choosing appropriate communication channels.
- The National Association of Secretaries of State #TrustedInfo2024 site[154]: NASS's public education effort to promote election officials as the trusted sources of election information.
- The National Association of State Election Directors FAQs[155]: NASED compiled Frequently Asked Questions to provide high-level information about election administration.
- The Harvard Kennedy School's Belfer Center publication, The Election Influence Operations Playbook[156]: A document to provide advice and guidance for election officials to assist them in better understanding, countering, and responding to influence operations.

33.4 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

33.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

[151] https://www.eac.gov/election-officials/communications-101

[152] https://www.eac.gov/sites/default/files/2024-05/Election_Official_Social_Media_Toolkit_508_Final.pdf

[153] https://www.youtube.com/playlist?list=PLwk7IuIKtO8bpSe5tAKbnO3_vlQ_gzLok

[154] https://www.nass.org/initiatives/trustedinfo

[155] https://www.nased.org/faqs

[156] https://www.belfercenter.org/publication/election-influence-operations-playbook-part-1

CHAPTER

THIRTYFOUR

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.

34.1 Goals

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

34.2 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[157] to guide your procurements.

34.3 Cost-Effective Tools

- CIS's A Guide for Ensuring Security in Election Technology Procurements[158]: Provides model procurement language that election officials can use to communicate their security priorities, better understand vendor security procedures, and facilitate a more precise cybersecurity dialogue with the private sector.

[157] https://learn.cisecurity.org/election-procurement-guide

[158] https://learn.cisecurity.org/election-procurement-guide

34.4 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)

34.5 Mapping to CIS Handbook Best Practices

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

CHAPTER

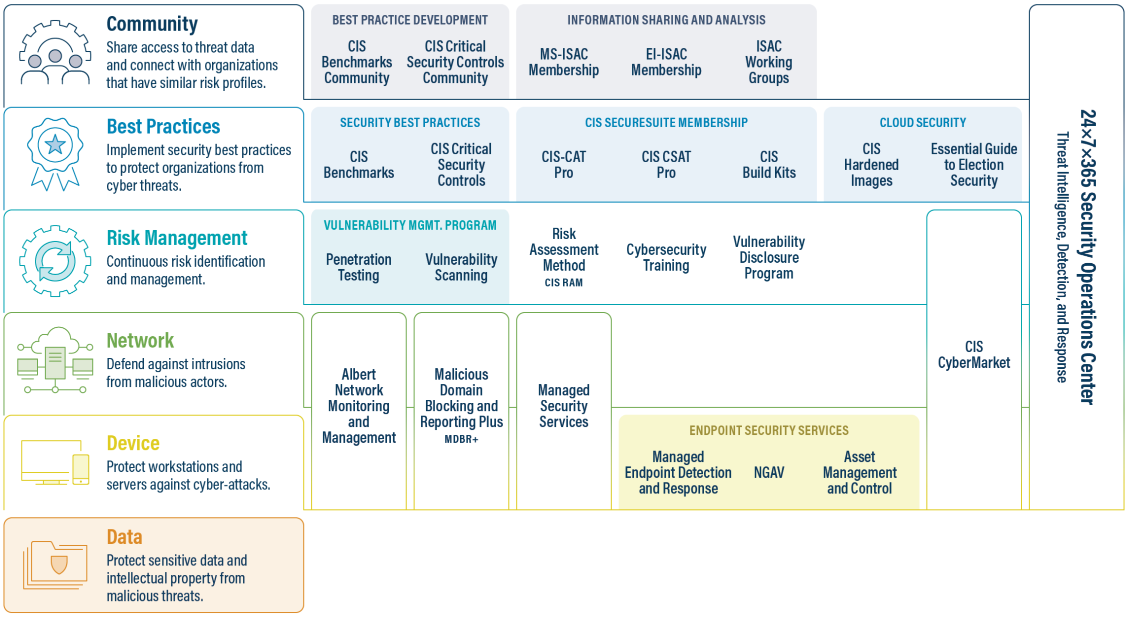
THIRTYFIVE

DEFENSE-IN-DEPTH

Defense-in-Depth is a comprehensive information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout your IT infrastructure to protect the confidentiality, integrity, and availability of that infrastructure and the data within.

No individual action can stop all cyber threats, so we increase security using multiple security mechanisms to mitigate against a wide variety of threats while incorporating redundancy in the event one mechanism fails. When successful, this approach significantly bolsters network security against many attack vectors. An effective defense-in-depth strategy typically includes the security best practices, tools, and policies in the graphic below, and can include many more depending on the maturity of the organization.

Defense-in-Depth Approach to Cybersecurity



Community
Share access to threat data and connect with organizations that have similar risk profiles.

BEST PRACTICE DEVELOPMENT: CIS Benchmarks Community; CIS Critical Security Controls Community

INFORMATION SHARING AND ANALYSIS: MS-ISAC Membership; EI-ISAC Membership; ISAC Working Groups

Best Practices
Implement security best practices to protect organizations from cyber threats.

SECURITY BEST PRACTICES: CIS Benchmarks; CIS Critical Security Controls

CIS SECURESUITE MEMBERSHIP: CIS-CAT Pro; CIS CSAT Pro; CIS Build Kits

CLOUD SECURITY: CIS Hardened Images; Essential Guide to Election Security

Risk Management
Continuous risk identification and management.

VULNERABILITY MGMT. PROGRAM: Penetration Testing; Vulnerability Scanning

Risk Assessment Method CIS RAM; Cybersecurity Training; Vulnerability Disclosure Program

Network
Defend against intrusions from malicious actors.

Albert Network Monitoring and Management; Malicious Domain Blocking and Reporting Plus MDBR+; Managed Security Services

Device
Protect workstations and servers against cyber-attacks.

ENDPOINT SECURITY SERVICES: Managed Endpoint Detection and Response; NGAV; Asset Management and Control

Data
Protect sensitive data and intellectual property from malicious threats.

CIS CyberMarket

24×7×365 Security Operations Center
Threat Intelligence, Detection, and Response

35.1 Goals

1. Set a foundation for your defense-in-depth journey by implementing cyber hygiene (Level 1 maturity)
2. Build toward a defense-in-depth posture by implementing baseline election priorities (Level 1 maturity)
3. Continually implement additional defenses by leveraging the Community Defense Model to prioritize your actions (Level 2 maturity)

35.2 Actions

For Defense-in-Depth, the necessary actions vary by maturity as detailed below.

35.2.1 Level 1 Maturity

Reaching a defense-in-depth cybersecurity posture takes time and resources, but begins with simple actions. For those organizations operating at a Level 1 maturity, this guide is built to help you begin and continually improve your cybersecurity posture.

1. Start a defense-in-depth journey by implementing cyber hygiene through the *baseline priority* (page 10) best practices.
2. Continue your journey by implementing this Guide's *baseline election priorities* (page 11).

35.2.2 Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, also detailed in this guide:

1. Implement additional defenses in a prioritized way by following this Guide's *prioritized best practices* (page 12) for your maturity level, based on the real-world, data-driven Community Defense Model.

35.3 Cost-Effective Tools

- The *CIS Controls* (page 94) can be a valuable resource for all organizations looking to systematically implement cyber defenses.

35.4 Mapping to CIS Controls and Safeguards

- The CIS Controls, taken together, collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

35.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

CHAPTER THIRTYSIX

ARTIFICIAL INTELLIGENCE IN ELECTIONS

Generative Artificial Intelligence (*AI*) is a technology that can create images, text, and videos with very little instruction from a user by learning patterns from very large datasets to predict the most likely response to a given prompt. For instance, text driven AI is trained on very large volumes of text, like blog posts, books, social media sites, and the like to learn how words and phrases are most likely to fit together. Similar approaches are used to "teach" AI how images should looked based on a text description, how a objects might relate to each other to look like natural movement. These technologies are advancing at a rapid pace, presenting opportunities and risks for individuals and society.

Like most tools and technologies, generative AI can be employed to improve and to harm election administration. "Deepfakes" are videos with recognizable people, such as an election official, but the actions and words of the people are created using generative AI. The same holds true for generating inaccurate news articles and social media content. OpenAI's ChatGPT[159] and Google's Bard[160] are generative AI platforms that create text based on a user's prompt. Another type of generative AI platform uses a text prompt to create images. Examples of this type of generative AI platform include Midjourney[161] and DALL-E[162].

Generative AI platforms pose a risk to elections due to their ability to quickly generate inaccurate information and other misleading materials. While there are benefits of generative AI, election officials need to be aware of the risks that generative AI poses on elections and implement safeguards to prepare for the 2024 presidential election year.

Dissemination of inaccurate information is generative AI's most apparent risk to elections. This technology can create inaccurate content that bad actors can then spread through other forms of media. Election officials have a lot to juggle on election day and the days leading up to an election. However, generative AI capabilities have the potential to make the job of election officials more difficult. Here are a few examples to explain how this can happen:

- Election officials work diligently to communicate information such as election deadlines, polling locations, and voting hours. With generative AI, media such as news articles, social media content, etc., can more quickly be generated and used to deceive voters and provide them with inaccurate information.

[159] https://chat.openai.com/auth/login

[160] https://bard.google.com

[161] https://www.midjourney.com/

[162] https://openai.com/dall-e-2

- Generative AI can create images and videos using a simple prompt. Generative AI platforms can be used to attack an election official's integrity by misrepresenting or fabricating a statement or act of an election official.
- Phishing emails are already a known cybersecurity threat. Generative AI can create convincing phishing emails that are nearly indistinguishable from a reputable email, elevating this threat.

As technology advances, generative AI platforms are becoming more intelligent. Therefore, it is important for election officials to be aware of new advances in generative AI so that they can take appropriate measures to mitigate it.

36.1 Goals

1. Know the definition of Generative AI (Level 1 maturity)
2. Understand the potential impact of Generative AI on election administration (Level 1 maturity)
3. Understand how to manage the additional risks presented by Generative AI (Level 1 maturity)

36.2 Actions

For Artificial Intelligence in Elections, the necessary actions are the same for all maturity levels.

Generative AI is a rapidly evolving technology in today's society, and, unfortunately, we cannot control it or avoid it. However, we can take measures to mitigate the potential effects of generative AI on elections. Here are a few recommendations:

1. Establish your office as a trusted source. Ensure the public knows where to go for accurate election information. Use your organization's website, social media platforms, local media, and press releases to accomplish this.
2. Monitor social media for inaccurate infomration and address it as your office sees fit.
3. Practice good cyber hygiene by implementing the best practices in this guide that *align with your maturity level* (page 4). Use strong passwords and multi-factor authentication. Also, include guidelines on generative AI platforms in your organization's cybersecurity policies.
4. Provide training. Generative AI technology is becoming more advanced each day. To stay educated, provide cybersecurity training to staff members including AI awareness and phishing campaign assessments. This reduces the risk of falling victim to AI.
5. Use available resources. Take advantage of CISA's Cybersecurity Toolkit to Protect Elections[163].

[163] https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections

36.3 Cost-Effective Tools

- CISA's Cybersecurity Toolkit to Protect Elections[164].

36.4 Mapping to CIS Controls and Safeguards

- CIS Controls associated with this best practices are addressed in the referenced actions

36.5 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

[164] https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections

CHAPTER

THIRTYSEVEN

PREPARING FOR ELECTION DAY DISRUPTIONS

Election Day disruptions pose significant risks to the integrity and stability of the electoral process. The primary aim of preparing for such disruptions is to ensure the safety and security of voters and election workers, maintain public confidence in the election process, and guarantee the continuity of election administration operations. Effective preparation involves establishing a robust preparedness and training baseline, developing comprehensive crisis communication strategies, and fostering coordination with local, state, and federal agencies. By proactively addressing potential threats and disruptions, election offices can mitigate risks, manage crises efficiently, and ensure that elections proceed with minimal interruptions.

Effective partnerships with local and state law enforcement are crucial for preparing and responding to Election Day disruptions. These partnerships ensure that election officials have access to the expertise, resources, and support needed to address security threats and maintain public safety. Collaborative efforts include joint training exercises, sharing critical information, and establishing clear communication protocols. By working closely with your local first responder community, election offices can develop comprehensive security plans, conduct risk assessments, and coordinate responses to potential threats effectively.

Similar to establishing partnerships with local and state law enforcement and emergency management officials, it is crucial to establish relationships with all relevant media outlets in your jurisdiction, including print, digital, and TV. In a crisis involving voting and public safety, transparency and communication are key. Identify points of contact for media outlets and cultivate these relationships to ensure your ability to provide the general public timely and relevant information during a crisis.

37.1 Have Collaborative Discussions

Effective collaboration between election officials and law enforcement is essential for creating a resilient relationship where both sides understand and support the other's mission. Law enforcement must recognize the critical importance of maintaining election operations continuity despite potential disruptions. Concurrently, election officials should understand that law enforcement views election disruptions through the lens of public safety and criminality. By establishing predefined roles and fostering mutual understanding, both parties can efficiently support each other's core mission objectives and ensure the electoral process's integrity while maintaining public safety.

Download and tailor CIS's `Guide for Collaborative Discussions on Election Disruption Preparedness` to help facilitate these discussions.

37.2 Examples of Election Day Disruptions

Bomb Threats

Bomb threats involve communications about the presence or intent to detonate explosives, causing disruptions, panic, and resource strain in election administration. These threats aim to disrupt or extort. Managing these threats requires assessing the threat, establishing communication protocols, and coordinating responses with law enforcement to ensure the safety of voters and election workers. While the use of "empty" bomb threats as a tactic of disruption has increased over the past several years, the use of actual bombs as a form of terrorism is still very real. All threats should be taken seriously validating the importance of coordinating with local law enforcement officials and other first responders.

Swatting

Swatting involves providing false information to law enforcement to trigger a tactical response by law enforcement, endangering election and law enforcement officials while also diverting resources from actual emergencies. While swatting has traditionally focused on individual targets, election-related disruptions may include the targeting of precinct locations, ballot counting facilities, and drop box locations. This both disrupts operations and poses significant safety risks. Preventing and mitigating swatting requires collaboration and information sharing with law enforcement.

White Powder Hazards

White powder incidents aim to cause fear and disrupt election administration operations. White powder hazards are most commonly sent via mail; however, the scattering of white powder at a polling location or dispersing it into or around a ballot drop box could disrupt voting and create fear among the electorate and election support staff. Preparation includes training staff to handle suspicious packages, maintaining communication channels, and having protocols for safe handling of mail to minimize disruptions and ensure voter and staff safety. White powder hazards can overwhelm the response capacity of local officials, particularly in smaller jurisdictions, making it essential to discuss this potential threat with your jurisdiction's first responders.

Other Election Day Disruptions

Election Day disruptions can include but are not limited to protests and counter-protests, active shooters, threats of violence, and other activities that, directly or indirectly, may interfere with the electoral process. These disruptions pose safety hazards, deter voter participation, and undermine the election's integrity. The risk of multiple simultaneous disruptions, such as a bomb threat coinciding with a protest outside the office, can complicate evacuation plans. Preparedness requires close coordination with law enforcement, fire, and emergency management officials; robust security measures at all election sites; and clear communication strategies. Having backup plans and effective communication with first responders is crucial to manage complex scenarios and ensuring the safety of voters and election workers.

37.3 Goals

1. Prepare your office for potential disruptions (Level 1 maturity)
2. Establish partnerships with local first responders and the community (Level 1 maturity)
3. Prepare and execute on your communications approach (Level 1 maturity)

37.4 Actions

For Preparing for Election Day Disruptions, the necessary actions are the same for all maturity levels.

37.4.1 Prepare your office

1. **Assign and Coordinate Roles**: Ensure clarity in duties for all staff during any potential disruptions.
2. **Appoint a Point of Contact (POC)**: Make someone in your office accountable for coordinating emergency contacts and responses.
3. **Budget Assessment**: Allocated resources to implement security and COOP plans.
4. **Develop a Detailed Security Plan**: Include protocols for managing various disruptions and consider using CISA's Protective Security Advisors program[165] for no-cost support.
5. **Brief Election Staff**: Provide all election staff with the knowledge and tools needed to respond effectively.
6. **Ensure COOP Readiness**: Develop, maintain, practice, and make a Continuity of Operations Plan (COOP) readily available. Consider the EAC Continuity of Operations Plan Template[166].

37.4.2 Prepare your partners and community

1. **Establish Initial Meetings**: Engage local law enforcement and security agencies to discuss collaboration and establish communication channels.
2. **Define External Partnership Scope**: Outline the scope and guidelines for a partnership with your local law enforcement counterparts. Consider creating a memorandum of agreement, ensuring a clear framework for cooperation.
3. **Conduct Joint Training and Exercises**: These can include simulations of various disruption scenarios, such as bomb threats or active shooter situations, ensuring that all parties understand their roles and responsibilities during a crisis.

[165] https://www.cisa.gov/sites/default/files/publications/CISA%2520Fact%2520Sheet%2520-%2520PSA%2520Program%2520-%2520508c_IAA%2520Final.19MAR2020.pdf

[166] https://www.eac.gov/sites/default/files/2023-09/EAC_COOP_Template_Final_508.pdf

4. **Share Information**: The locations of polling places and contact information for key personnel helps law enforcement plan and respond more effectively to incidents.
5. **Establish Communication Protocols**: Ensure swift and appropriate responses by designating points of contact and using secure communication channels.

37.4.3 Prepare your communications approach

1. **Internal Communication**: Cross-train staff for multiple roles and establish protocols for different disruptions using email, phone, text, or in-person communication to keep staff informed in real-time.
2. **External Communication**: Establish a communications point of contact and ensure law enforcement counterparts have POCs. Develop joint communication protocols with law enforcement for coordinated responses and to avoid conflicting statements.
3. **Establish Relationships with Media Outlets**: Ensure local media know who they will hear from for authentic information. Include print, radio, television—anywhere your constituents' get information.
4. **Enhance Online Presence**: Establish accounts as official to so the media and public know where to get factual information.
5. **Leveraging Multiple Channels**: In a crisis, communicate through ever means available to you.
6. **Pre-approve Messaging**: While every emergency is unique, have approve template for potential crises to shorten your response time and get ahead of rumors and falsehoods.
7. **Engage the Community**: Build trust and cooperation between election officials, law enforcement, and the public to enhance overall preparedness and ensure a more coordinated response to disruptions.
8. **Post-Election Review**: Review, discuss, and update plans after every election. Consider using The Elections Group Crisis communications toolkit.

37.5 Cost-Effective Tools

- EAC's Continuity of Operations Plan Template[167].
- CISA's Training Video Series[168].
- CISA's Last Mile Toolkit[169].

[167] https://www.eac.gov/sites/default/files/2023-09/EAC_COOP_Template_Final_508.pdf
[168] https://www.cisa.gov/resources-tools/resources/what-do-training-video-series
[169] https://www.cisa.gov/sites/default/files/2024-01/Last%20Mile%20Toolkit%20%28Letter%20Size%29.pdf

37.5.1 Learn More

- CISA's Ballot Drop Box Security Best Practices for Incendiary Devices[170].
- The Elections Group Strategies for Increasing Dropbox Security[171].
- CIS's `Guide for Collaborative Discussions on Election Disruption Preparedness`.
- CISA's Bomb Threat Guide[172].
- CISA's Swatting Prevention and Response Guidance[173].
- CISA's best practices for mail screening[174].
- CISA's Enhancing Election Security Through Public Communications[175].
- The Committee for Safe and Secure Elections Resources for Election and Law enforcement Officials[176].
- The Elections Group de-escalation resources[177].

37.6 Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls

37.7 Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

[170] https://www.cisa.gov/resources-tools/resources/ballot-drop-box-security-best-practices-incendiary-devices
[171] https://electionsgroup.com/resource/7-strategies-for-enhancing-ballot-drop-box-security/
[172] https://www.cisa.gov/sites/default/files/2023-08/Bomb%20Threat%20Guide_v1.0.pdf
[173] https://www.cisa.gov/sites/default/files/2024-05/Swatting%20Guidance%20for%20Election%20Workers%20and%20Law%20Enforcement.pdf
[174] https://www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf
[175] https://www.cisa.gov/sites/default/files/2024-06/Enhancing%20Election%20Security%20Through%20Public%20Communications_508c.pdf
[176] https://safeelections.org/resources
[177] https://electionsgroup.com/resource/de-escalation/

CHAPTER THIRTYEIGHT

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* (page 114): Information about the structure of the document, its history, and its relevance to CIS's Handbook for Election Infrastructure Security.
2. *How To* (page 118): Information on the best uses and most effective ways to work with the Guide to achieve that which you wish to accomplish.
3. Small Jurisdiction *Worksheets* (page 119): A set of downloadable worksheets for use at the Level 1 maturity level.
4. For legacy purposes, a *mapping* (page 121) of the best practices to the best practices from the Handbook for Election Infrastructure Security.

In addition to the appendices, there is an informative *election infrastructure primer* (page 130), to give background on the architecture of election systems, the role information technology, risks and threats.

There is also a *glossary* (page 151) of technical terms used throughout the Guide and an *acronym* (page 153) list.

CHAPTER THIRTYNINE

ABOUT THE ESSENTIAL GUIDE TO ELECTION SECURITY

When The Handbook for Election Infrastructure Security[178] 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.

39.1 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. In 2021, CIS 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.

[178] https://www.cisecurity.org/elections

39.2 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.

CIS 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. CIS has greatly increased the number of freely available tools and services for election offices across the country.
3. Since releasing the Handbook, CIS has developed a series of best practice guides[179] 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[180] (*CISA*) and other government agencies; and
   - A body of work for other academic and nonprofit organizations such as the *Global Cyber Alliance <https://gcatoolkit.org/elections/>*, 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. Managing inaccurate information about election administration has become one of the thorniest and most pervasive threats to democracy and election officials need guidance on addressing inaccurate information and threats and harassment of election officials.

[179] https://www.cisecurity.org/elections

[180] https://www.cisa.gov/election-security

39.3 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* (page 4) section.
2. We've incorporated new best practices that cover the many threats and opportunities that have emerged, like around managing inaccurate information about election administration, understanding artificial intelligence in elections, and how to access 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* (page 114), 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.

39.4 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

FORTY

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

FORTYONE

LEVEL 1 WORKSHEETS

This page links to a set of worksheets for use at the Level 1 maturity level. There is one Excel format[181] file to download that contains all ten worksheets.

Completing these worksheets provides the *baseline priorities* (page 10) for Level 1.

A organization at the Level 1 maturity should still complete the Level 1 *election priorities* (page 11).

There are ten total worksheets in one file. Download the full set of worksheets in Excel format[182].

41.1 IT Inventory Worksheets

Within the Excel format[183] 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* (page 24) 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

41.2 Cybersecurity Action Worksheets

Within the Excel format[184] 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* (page 11).

1. Asset protection

[181] https://docs.cisecurity.org/en/latest/_worksheets/EGES_level_1_baseline_wksts.xlsx
[182] https://docs.cisecurity.org/en/latest/_worksheets/EGES_level_1_baseline_wksts.xlsx
[183] https://docs.cisecurity.org/en/latest/_worksheets/EGES_level_1_baseline_wksts.xlsx
[184] https://docs.cisecurity.org/en/latest/_worksheets/EGES_level_1_baseline_wksts.xlsx

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

CHAPTER

FORTYTWO

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)	Encrypt Data in Transit

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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	
12	Ensure critical data are encrypted and digitally signed	• Encrypt Data at Rest • Encrypt Data in Transit
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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
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	

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
53	Ensure all workstations and user accounts are logged off after a period of inactivity	
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
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	
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

continues on next page

Table 1 – continued from previous page

Handbook BP #	Handbook Best Practice Title	Essential Guide Best Practice
84	Ensure critical data is encrypted and digitally signed	• Encrypt Data at Rest • Encrypt Data in Transit
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

This section draws from the Handbook for Election Infrastructure Security. It is an informative section to help understand and conceptualize how the various election technology components work and interact. While this Essential Guide to Election Security is our recommended go-to for best practices, you can still download the Handbook[185].

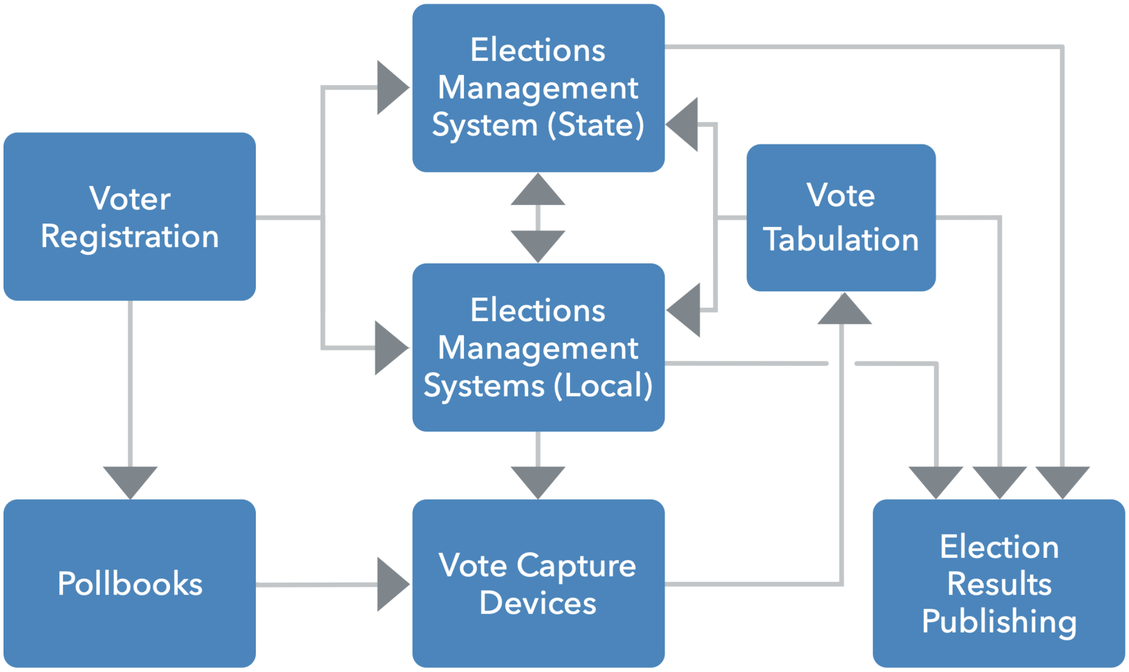
[185] https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

A PRIMER ON ELECTION INFRASTRUCTURE SECURITY

There are many flavors of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. Poll worker management systems, results publishing, and many other systems all have to come together, often requiring a careful orchestration of many systems provided by many vendors. As the joke goes, "there's no easy way to describe an election process in a single graphic without leaving someone out or making somebody unhappy."

That said, many experts have studied the election processes at length, and there are several fundamental components common to nearly all elections systems in the United States.

In some jurisdictions, the owner of various aspects of the architecture may differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices, though there are often additional business processes and practices that help mitigate risk.


Elections Management System (State)
Voter Registration
Vote Tabulation
Elections Management Systems (Local)
Pollbooks
Vote Capture Devices
Election Results Publishing

Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components may exist at the state level, at the local level, or both, and some will not be applicable in certain jurisdictions. Even where there is a substantial amount of legacy infrastructure—-old systems that are difficult or impossible to update—-much can be done to mitigate risks. These systems are described below and appropriate best practices and actions are provided throughout this Guide.

The next section describes the *connectedness* (page 132) of election systems, to help understand and conceptualize how various types of election technology are (or are not) connected to each other, the internet, and other networks.

The remainder of the sections give background on the architecture of election systems, the role information technology, the risks and threats for each, and how they connect in the context of cybersecurity risk management. Importantly, this primer gives information about protecting the infrastructure. There are many process-oriented risk mitigations employed throughout election administration that are not addressed here.

CHAPTER

FORTYFOUR

ELECTION SYSTEMS AND THEIR NETWORK CONNECTIONS

Any given piece of election technology fits into one of three classes of “connectedness” based on how they interact with networks, other systems, and the internet. This connectedness is extremely influential in the overall risk profile–the types of attacks the technology might face–and thus is a good starting point for threat modeling.

While there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analyzing the manner in which they connect to networks and other devices.

The three connectedness classes are:

1. **Network connected systems and components**. Network connected components are interconnected with other devices to achieve their objectives, whether through the internet or internal networks, hardwired or WiFI or Bluetooth. The level of interconnection, while providing various benefits, also introduces additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means organizations must make extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. Examples include:

   - Digital voter registration systems.
   - Election results transmission via cellular modems or the plain old telephone system.
   - An Election Management System (EMS) connected to a private county network.

2. **Indirectly connected systems**. Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, have to exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives. While the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive. Examples include:

   - Using a USB stick to transfer ballot definitions and other election information to a vote capture device such as a ballot marking device.

  - Using write-once removable media to transfer precinct definitions from a networked machine to an election management system.

3. **Non-digital elections components**. These are aspects of the elections process that have no digital component but still may face relevant risks through business processes. An example would be the mailing, completing, and returning of a paper mail-in ballot. While aspects of the overall process—-such as an online request for a ballot–may leverage digital infrastructure, the aspect of this process that is purely paper-based does not face the same cybersecurity risks.

44.1 Transmission between components creates vulnerabilities

While securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack, lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected.

For instance, while paper pollbooks wouldn't typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks that must be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e., vote capture) devices. These transmission risks must also be managed.

CHAPTER

FORTYFIVE

VOTER REGISTRATION

Every state has a unique approach to voter registration —- including some states with automatic voter registration[186] —- but there are several commonalities shared by all of them. Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks—paper and electronic—as well as provide information back to the voter as they verify their registration and look up polling locations and sample ballots.

The inputs to voter registration systems are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of an individual), and record updates, most often due to an individual moving within the state. The outputs include facilitating voter lookups—-such as a voter verifying they are registered, seeking a sample ballot, or finding their polling place—-and transfer of voter information to pollbooks. By their nature, that means voter registration systems are not only critical to election administration, but include personal information such as name, birth date, and postal address.

In each of these cases, there is a master voter database at the state level. This database is populated in one of three broad ways (lightly edited from the Election Assistance Commission's 2014 Statutory Overview[187]):

1. A top-down system in which the data are hosted on a single, central platform of hardware and maintained by the state with data and information supplied by local jurisdictions,
2. A bottom-up system in which the data are hosted on local jurisdictions' hardware and periodically compiled to form a statewide voter registration list, or
3. A hybrid approach, which is a combination of a top-down and bottom-up system.

For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on commercial-off-the-shelf (*COTS*) hardware, software, and cloud services. Because they use these common computing platforms, voter registration systems may be part of a shared computing system, though in many cases they are dedicated systems with dedicated software.

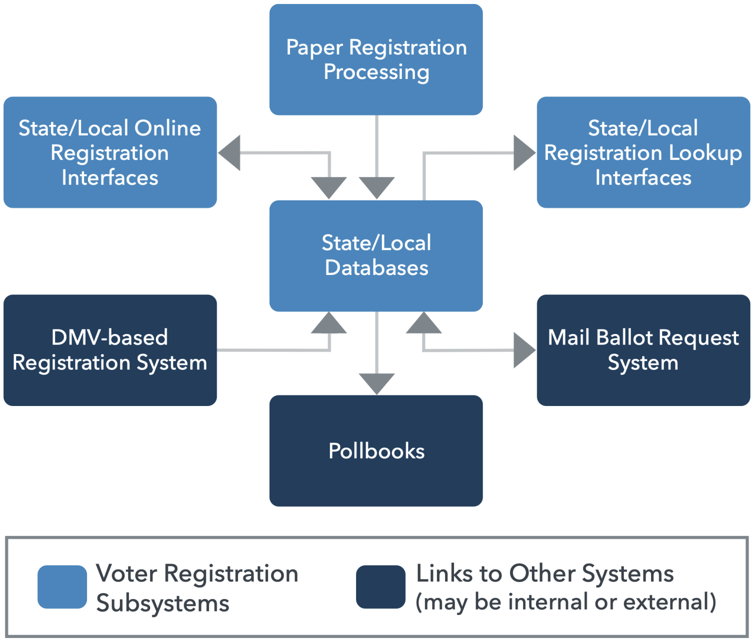
While jurisdictions vary in how they allow voters to apply or update their registration, in many states, the most common way voters access a registration system is through the state's department of motor vehicles (DMV). Additionally, voters' connection to the voter registration system may

[186] https://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx

[187] https://www.eac.gov/sites/default/files/eac_assets/1/1/2014%20Statutory%20Overview_Final-2014-05-15.pdf

run through direct means such as a county or state registration portal, or through indirect means like mailing in a registration on paper. To address this risk, many voter registration systems with which the voter would interact are separated from the "official," or production, voter registration system. Periodically, a report of changes is generated and undergoes a quality assurance review that must be certified before being entered into the production system. This can substantially reduce, for instance, an online portal as a vector of attack, though the production system may still be network connected in other ways.

In general, voter registration systems exhibit the risk characteristics of a general-purpose computing system and, more specifically, any network connected database application. To properly mitigate risks, each voter registration system within a state, and links to the voter registration system, needs a comprehensive assessment of its technical characteristics and the application of appropriate security controls.


Paper Registration Processing
State/Local Online Registration Interfaces
State/Local Registration Lookup Interfaces
State/Local Databases
DMV-based Registration System
Mail Ballot Request System
Pollbooks
Voter Registration Subsystems
Links to Other Systems (may be internal or external)

45.1 Types of voter registration systems

Voter registration generally occurs in one of two ways, each of which is recorded in a statewide registration system.

1. Online registration: a website or other web application allows prospective voters to register electronically and have election officials review their registration for validity, which, if valid, is entered into the voter registration database. Same-day registration, because of the need for live updating and cross checking, usually falls into this category.

2. Paper-based registration: prospective voters submit a paper voter registration form that is reviewed by election officials and, if valid, entered into the voter registration database.

The type of voter registration employed at DMVs will vary by state—and perhaps locality—but should typically be viewed as a form of online registration.

45.2 Risks and threats

As noted in the previous section, the ability to access voter registration systems through the internet results in a significant increase in vulnerability and resulting risk. There are well known best practices to mitigate these risks (see many of the best practices in this Guide, especially *here* (page 33) and *here* (page 50)), but the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components.

While attacks on voter registration systems may have a specific purpose not found outside the elections domain, the vectors for those attacks, and thus the primary risks and threats associated with voter registration systems, are similar to those of other systems running on COTS IT hardware, software, or cloud systems, and include:

- Risks associated with established (whether persistent or intermittent) internet connectivity;
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities;
- Security weaknesses in the underlying COTS products, whether hardware, software or cloud systems;
- Errors in properly managing authentication and access control for authorized users;
- Difficulty associated with finding, and rolling back, improper changes found after the fact;
- Infrastructure- and process-related issues associated with backup and auditing; and
- Vulnerabilities resulting from misconfigurations.

These items must be managed to ensure proper management of voter registration systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats, as provided throughout this Guide and in related cyberscurity guidance such as the *CIS Controls* (page 94).

45.3 How these components connect

Each type of voter registration, along with the master voter registration database, should have risks evaluated individually based on its type of connectivity and employ controls and best practices found throughout this Guide that correspond to the type of connectivity and are appropriate to address risks. That said, aspects of the voter registration systems, and the types that may be implemented, have general characteristics that can be classified by connectivity.

Table 1: Connection Types for Voter Registration Systems

Connectedness	System Type and Additional Information
Network Connected	Online Registration. In addition, the master registration database, system itself, and online voter lookups should be considered network connected.
Indirectly Connected	Not applicable in most voter registration implementations.
Not Connected	Paper-based registration.
Additional Transmission-based Risks	Transmission of a registration via email or fax leverages a digital component.

CHAPTER

FORTYSIX

POLLBOOKS

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today and are common as a backup strategy, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this section focuses primarily on electronic pollbooks (epollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These epollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These epollbooks are most often dedicated software built on COTS hardware (usually a tablet) and riding on COTS operating systems, like Android or iPadOS, though laptops with Windows or MacOS are still in use as well.

The primary input to epollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, epollbooks may require additional inputs and outputs to allow for election day changes. A proper record of a voter voting is critical, both auditing and properly giving "credit" to the voter; some states remove voters from the rolls if they go too long without having cast a ballot.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer—whether at the state or local level, or via commercial printing services—protects the integrity of the information in printed pollbooks.

46.1 Risks and threats

Attacks on epollbooks would generally serve to disrupt the election day process by one of these three situations:

1. Attacking the integrity of the data on the pollbook by altering the information displayed from voter rolls,
2. Disrupting the availability of the epollbooks themselves, or
3. In some cases, causing issues with the vote capture device by altering an activation token.

Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that causes delays in their casting a ballot or forces them to use the provisional ballot process, but could also occur in the epollbooks themselves and during the transmission of data to the epollbook.

An epollbook may or may not be connected to a network. If they are network connected, they must be treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an epollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for epollbooks,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact.

These risks must be managed to ensure proper management of pollbooks. Because most are risks and threats shared among users of COTS products more broadly than in elections, there is a well-established set of controls to mitigate risk and thwart threats.

46.2 How these components connect

Managing risks associated with epollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data.

Table 1: Connection Types for Pollbooks

Connectedness	System Type and Additional Information
Network Connected	Pollbook connects via a wired or wireless network
Indirectly Connected	Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).
Not Connected	Paper-based pollbooks.
Additional Transmission-based Risks	Transmission of data for paper-based pollbooks for formatting or printing.

CHAPTER

FORTYSEVEN

STATE AND LOCAL ELECTION MANAGEMENT SYSTEMS

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A state EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of this handbook, vote tabulation is broken out into its own section.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties between the state and the local jurisdictions and the manner in which each state or local jurisdiction handles particular aspects of the election process.

47.1 Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

The consequences of a successful attack in an EMS are significant. These include the inability to properly control election processes and systems or, depending on the functions of the EMS, in-correct assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

To help manage these risks, most election offices do not have network connections to their EMS, and rarely have internet connections. Instead, they keep the EMS isolated as a standalone machine or on a separate network that has no internet connection and is solely dedicated to the functioning of the EMS. Data transfers to and from the EMS are conducted with removable media only. This is an indirect connection and presents a particular set of risks to mitigate.

47.2 How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a state or local EMS is network connected, communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP), or all data is transferred through removable media.

Table 1: Connection Types for Election Management Systems

Connectedness	System Type and Additional Information
Network Connected	Unless known definitively to have no network capabilities, treat an EMS as network connected.
Indirectly Connected	If known definitively to have no network capabilities, treat an EMS as indirectly connected.
Not Connected	Not applicable.
Additional Transmission-based Risks	Not applicable.

CHAPTER FORTYEIGHT

VOTE CAPTURE

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place may give voters the choice of electronic ballot marking devices or paper ballots. Additionally, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

Because of this diversity in vote capture approaches, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other federal partners, state and local governments, vendors, and others in the elections community, maintain standards and a certification program[188] for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a set of threats, risks, and categorizations to help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security-—and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

The primary inputs to vote capture devices are the ballot definition file, which describes to the device how to display the ballot, an activation key (for some electronic machines), and the ballot itself for scanning of a paper ballot. The primary output is the cast vote record.

In cybersecurity, we often talk about non-repudiation: the inability to deny having taken an action. Our democracy is founded in the opposite principle: your ballot is secret; no one should be able to prove who or what you voted for or against in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. We intentionally create voter anonymity through a breakpoint between the fact that an individual voted and what votes they actually cast. We never want to enable the ability to look at a marked ballot and track it back to a specific voter.

Instead, we must carefully protect the integrity and secrecy of the vote cast through the capture process and into the process of tabulation. To do this, best practices call for applying a series of

[188] https://www.eac.gov/voting-equipment/testing-and-certification-program

controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

48.1 Types of vote capture processes

Vote capture generally occurs in one of six ways:

1. *Voter marked and hand counted paper balloting*. Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.

2. *Voter marked paper balloting with scanning*. Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots. These scanners have several flavors, with the most common being: precinct count optical scanners (*PCOS*), central count optical scanner (*CCOS*), and simply optical scanners (*OS*).

3. *Electronic marking with paper ballot output*. Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These types of machines are referred to as ballot marking devices (*BMD*). These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a ballot marking device.

4. *Electronic voting with paper record*. The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a direct record electronic (*DRE*) device with voter verifiable paper audit trail (*VVPAT*).

5. *Electronic voting with no paper record*. The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as just a DRE.

6. *Electronic receipt and delivery of ballots conducted remotely*. The majority of ballots received by voters using this method are voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (*UOCAVA*). Though most UOCAVA votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. Voting methods

commonly called internet voting or mobile voting fall under this process.

48.2 Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject—in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, a state or local entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The last type of vote capture described above, *'electronic receipt and delivery of ballots conducted remotely'* can take on a large number of flavors. In terms of cybersecurity-related risks, for activities like emailing marked ballots, election officials must consider especially risks involved in the transmission of the ballot. If the transmission of the marked ballot is done via digital means, it is subject to the risks of that transmission mode.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- If ever networked, risks associated with established (whether persistent or intermittent) network connectivity,
- Risks associated with the corruption of removable media or temporary physical connections to systems that are networked,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

48.3 How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity.

The numbering in the right column below align with the types of vote capture processes above.

Table 1: Connection Types for Vote Capture

Connectedness	System Type and Additional Information
Network Connected	If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered network connected. Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network. Also, many central count scanners, used for Voter marked paper balloting with scanning in batches (usually vote by mail ballots) are similarly networked on a closed-LAN. Some electronic vote capture machines also directly transmit data for election night reporting.
Indirectly Connected	Type 2: *Voter marked paper balloting with scanning*. Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Type 3: *Electronic voting with paper ballot output*. In addition to the role of the scanners, the vote capture machines are typically not network connected, but must be programmed to display the ballot and print the ballot in the correct format. Type 4: *Electronic voting with paper record*. The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Type 5: *Electronic voting with no paper record*. The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Note: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered network connected.
Not Connected	Type 1: *Voter marked and hand counted paper balloting*. Out of scope in this handbook as the vote capture process does not include a digital component.
Additional Transmission-based Risks	Type 6: *Electronic voting conducted remotely*. These methods vary greatly and must be addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations.

CHAPTER

FORTYNINE

VOTE TABULATION

Vote tabulation is the aggregation of votes (e.g., cast vote records and vote summaries) for the purpose of generating totals and results report files. Many distinguish between vote tabulation and vote aggregation. Most commonly, the former is totalling of votes from various machines by a precint, and the latter totalling of votes from precincts by the jurisdiction. For the purposes of this section, we treat them synonymously.

This section on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Here, vote tabulation is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

49.1 Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g., results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across a network. Vote data is most often transferred across jurisdictions and to the state through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,

- Errors in properly managing authentication and access control for authorized users,
- Lack of confidentiality and integrity protection for transmitted results,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These primary risks must be managed to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

49.2 How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network.

Table 1: Connection Types for Vote Tabulation

Connectedness	System Type and Additional Information
Network Connected	In some cases, vote tabulation equipment will be network connected, whether through a wired or wireless connection.
Indirectly Connected	If vote tabulation equipment is not network connected, it is indirectly connected through removable media.
Not Connected	Not applicable.
Additional transmission-based risks	Not applicable.

CHAPTER

FIFTY

ELECTION RESULTS REPORTING AND PUBLISHING

After voting is completed, results must be communicated both internally and to the public. The approach to doing this varies widely but the goal is the same: getting accurate results out as quickly as possible. The time it takes to do this depends on many factors, including state laws around where and how results are counted and when results can be posted, the length of lines when the polls close, technical specific of reporting, and factors like whether there are multiple time zones in a jurisdiciton. For instance, a state may specify that mail in ballots cannot even be opened until after polls close, which can create a signficint lag in results reporting.

This section focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing are tabulated votes, as described in the previous section. The systems used for reporting and publishing are likely networked, and, in many cases, have public facing websites or application program interfaces (APIs).

The outputs are the unofficial election results, typically published on a website, often in multiple formats such as extensible markup language (XML), hypertext markup language (HTML), portable document format (PDF), and comma-separated values (CSV). There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results may be kept on a system that is not persistently connected to the internet.

50.1 Risks and threats

As noted earlier, the consequences of an attack that would impact unofficial election results reporting and publishing could be significant, resulting in loss of confidence in the correctly reported election results when they are finally posted. The primary risks to election reporting and publishing, when connected devices are used to transmit data and communicate results, are similar to those of other COTS systems. Such risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,

- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

50.2 How these components connect

Depending on the approach to submitting tabulated votes, the reporting component may be network connected. The publishing component is almost certainly network connected, but may be indirectly connected, depending on the implementation.

Table 1: Connection Types for Vote Tabulation

Connectedness	System Type and Additional Information
Network Connected	In some cases, election night reporting will be network connected, whether through a wired or wireless connection. The publishing component of election night reporting is almost certainly network connected, whether through a wired or wireless connection.
Indirectly Connected	If the election night reporting process is not network connected, it is indirectly connected through removable media.
Not Connected	Not applicable.
Additional transmission-based risks	Not applicable.

CHAPTER FIFTYONE

GLOSSARY

NIST's Computer Security Resource Center Glossary[189] 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[190]. 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[191].

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.)

generative artificial intelligence a technology that can create images, text, and videos with very little instruction from a user by learning patterns from very large datasets to predict the most likely response to a given prompt

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

[189] https://csrc.nist.gov/glossary/

[190] https://www.cve.org

[191] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

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.

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.

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

CHAPTER FIFTYTWO

ACRONYMS

NIST's Computer Security Resource Center Glossary[192] is a useful reference for information security terms, acronyms, and organizations.

AES Advanced Encryption Standard

AI artificial intelligence

BMD ballot marking device

CCOS central count optical scanner

CDM *Community Defense Model*

Continuous Diagnostics and Mitigation (Common)

Continuous Diagnostics and Monitoring (Old)

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

COTS commercial-off-the-shelf

CSF NIST Cybersecurity Frameowrk

CVE *Common Vulnerabilities and Exploits*

CVSS Common Vulnerability Scoring System

DNS domain name system

DRE direct record electronic

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

[192] https://csrc.nist.gov/glossary/

EMS election management system

GRC governance, risk, and compliance

IDS intrusion detection system

IG Implementation Group

IPS intrustion prevention system

IT information technology

MDBR *Malicious Domain Blocking and Reporting*

MDM mobile device management

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

OS optical scanner

PCMCIA Personal Computer Memory Card International Association

PCOS precinct count optical scanner

PII personally identifiable information

US-CERT United States Computer Emergency Readiness Team

UOCAVA Uniformed and Overseas Citizens Absentee Voting Act

USB universal serial bus

VDP vulnerability disclosure program

VPN virtual private network

VVPAT voter verifiable paper audit trail

WPA wi-fi protected access

INDEX

A

AES, 153
AI, 153
authentication, 151

B

BMD, 153

C

CCOS, 153
CD-R, 153
CDM, 153
CFAA, 153
CIS, 153
CIS Controls, 151
CISA, 153
common vulnerabilities and exploits, 151
Community Defense Model, 151
COTS, 153
CSF, 153
CVE, 153
CVSS, 153

D

DNS, 153
domain name system, 151
DRE, 153
DVD-R, 153

E

EAC, 153
EDR, 153
EI-ISAC, 153
EMS, 154
encryption, 151
endpoint detection and response, 151
endpoint protection, 151

G

generative artificial intelligence, 151
GRC, 154

H

hashing, 151

I

IDS, 154
IG, 154
Implementation Group, 152
IPS, 154
IT, 154

M

malicious domain blocking and reporting, 152
malware, 152
MDBR, 154
MDM, 154
MFA, 154
MS-ISAC, 154
multi-factor authentication, 152

N

NCSR, 154
NIST, 154
NIST SP, 154
NVD, 154

O

OS, 154

P

patching, 152
PCMCIA, 154
PCOS, 154
PII, 154

R

ransomware, 152

S

salting, 152

U

UOCAVA, 154
US-CERT, 154
USB, 154

V

VDP, 154
virtual private network, 152
VPN, 154
VVPAT, 154

W

WPA, 154