CIS® **Center for Internet Security**®

A Handbook for

Elections Infrastructure Security

About CIS

CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

Center for Internet Security®

| 31 Tech Valley Drive | T: 518.266.3460 | www.cisecurity.org |
| East Greenbush, New York 12061 | F: 518.266.2085 | Follow us on Twitter @CISecurity |
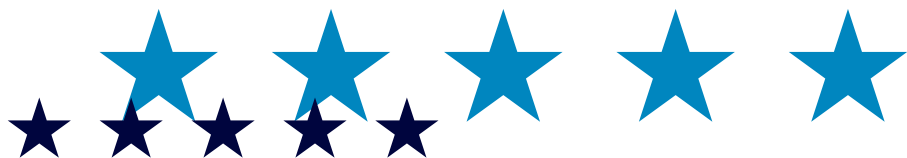
A Handbook for

Elections Infrastructure Security

Part 1:
Introduction

Part 2:
Elections Systems and Risk

Part 3:
Mitigating System Risk

https://www.cisecurity.org/elections-resources/

Acknowledgments

Part 1: **Introduction**

How cybersecurity and elections intersect and why it matters.

To enable the elections that define democracy, we must protect the security and reliability of elections infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand what to focus on, know how to prioritize and parse the enormous amount of guidance available on protecting information technology (IT) systems, and engage in additional collaboration to address common threats to this critical aspect of democracy.

The Center for Internet Security (CIS) and its partners publish this handbook as part of a comprehensive, nationwide approach to protect the democratic institution of voting. Election officials have been working diligently to secure their systems but, like so many other sectors, the threat to national security rises above any individual organization; we can accomplish more together, and we all share the same goal of free and fair elections. To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a national response to threats against elections infrastructure. This handbook addresses cybersecurity-related aspects of elections systems.

Background and purpose

Elections are the bedrock of democracy. Even before the establishment of the United States, adversaries sought to corrupt, interrupt, or otherwise disrupt democracy by subverting elections. From adversarial nation states, to terror groups, to Boss Tweed vote strikers, to those simply wishing to wreak havoc, attacks on the voting process are as old as voting itself. There is no way around it: protecting democracy calls for protecting elections.

The desire of some to disrupt elections has not changed; Joseph Harris's 1934 seminal book on elections, *Election Administration in the United States,* enumerates a series of election fraud incidents throughout American history. What is different in recent years is some of the tactics of such efforts to undermine democracy. Attacks leveraging weaknesses in digital infrastructure now augment traditional approaches and have become an increasingly common approach.

Judging by activity in industries and sectors outside elections, this should come as no surprise. Organizations across all sectors and government entities alike face daily attacks from actors with widely varying levels of sophistication. The most capable, best protected organizations have specific plans for addressing evolving threats. The plans are never static; these entities continually adapt—as do their adversaries—requiring an ongoing investment in security.

Moreover, in many industries and sectors, the good guys have realized that a go-it-alone strategy isn't enough. They've developed approaches that allow them to share information, establish best practices, and develop coordinated response plans to mitigate effects of coordinated attacks. This collaboration raises the level of security for the individual organizations, their respective industries or sectors, and the country.

Even in the financial services industry—in which annual investments by individual organizations in improved security for their digital systems can range in the many hundreds of millions of dollars—organizations pool some resources to support the Financial Services Information Sharing and Analysis Center. This collaborative approach to monitoring the evolving threat environment helps support even the most substantial individual efforts. These same approaches have been repeated in many industries, including communications, the defense industrial base, aviation, oil and gas, real estate, electricity, and others. Protecting elections infrastructure is certainly no less important to our country's national security and overall well-being than protecting the infrastructures in these other vital sectors.

In the state and local sector, the Multi-State Information Sharing & Analysis Center (MS-ISAC) works with state and local entities to monitor threats to their systems, detect common attacks across states, and support mitigation of risks presented by vulnerabilities and changing attacker behavior. This results in a more rapid deployment of solutions when new threats emerge; if there's one thing we know about these actors, once they succeed in an attack, they'll duplicate it everywhere they can.

The parent organization of the MS-ISAC and sponsor of this handbook, CIS, has used collaboration among a large number of security experts as a means to identify best security practices. These collaborative processes have resulted in several products available to state and local governments and other entities, including election officials and their technical staff. These include the CIS Controls and CIS Benchmarks, which heavily inform the recommendations in this handbook.

An underlying reality to all current work in cybersecurity is that a skills gap exists for cybersecurity globally, across all industries—elections included. Closing this skills gap is critical to elections and securing the process. Implementing best practices is only possible with the right people who have the necessary skill-set. Therefore, we hope what follows in this handbook will serve individuals with differing skills and resources in implementing practical guidance for election administration.

The elections environment

Elections in the United States are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the federal government provides some laws and regulations, states have substantial discretion on the process of conducting elections. The federal government does not administer elections and has a limited role in dictating how the process is to be conducted.

States act as the primary authority for the laws and regulations that govern the process of conducting an election in that state. Under federal law, states must designate a chief state election official. This official typically sets rules and regulations for the implementation of election technologies and their use. Although states are heavily involved in setting the rules and policies for administering elections, and in choosing election technology, in most states local jurisdictions administer and conduct the processes of an election.

Many local jurisdictions have the ability to procure their own election technology from a set of certified or approved manufacturers and vendors designated by their respective state. Additionally, the local jurisdictions are typically responsible for inventorying, securing, and training staff on those technologies. Depending on the size and resources of the jurisdiction, the number and technical skills of the staff can vary greatly, ranging from an elections team with its own dedicated IT and security personnel to a single person with little to no IT background. Many elections offices rely on IT resources shared with other administrative functions (e.g., other county agencies) or rely exclusively on technology providers (e.g., elections and IT systems vendors) for implementing and securing their election infrastructure. This can result in dependencies that are outside of the local officials' control.

Audience

By using this handbook, we hope election officials and those that manufacture, own, operate, or are otherwise involved with elections systems and their IT components are better able to understand and prioritize risks, understand best practices that can identify threats, detect attacks, allow for recovery from cybersecurity incidents, and, ultimately, continue to provide and support systems for the execution of free and fair elections.

In addition to this handbook providing a path to continually evolving security, perhaps the most important aspect of this effort is to help instill a continued sense of faith in elections by voters themselves. We hope election officials are able to use this handbook to highlight the past and ongoing work they've done to secure the elections process and that, through openness, transparency, inclusion of relevant stakeholders, and consideration of the entirety of the elections process, voters recognize that democracy is working and their votes will count.

More specifically, we hope this handbook is of use to each of the following:

- **Election officials and senior executives.** These individuals are accountable for executing elections. In addition to state and local election officials, they may include those indirectly involved in the election process, such as the offices of legislators and governors.
- **Owners and operators of elections systems.** These individuals have more responsibility for the systems themselves, though there may be some overlap with election officials. It's critical that they understand the risk context and the technical guidance in this handbook.
- **Vendors of hardware and software.** Whether providing systems and services dedicated to elections or general purpose but used in elections, vendors are, and must remain, partners in this process. Moreover, vendors often provide the primary technology expertise and labor to local election officials. Vendors have a vested interest in their products and services, and election officials driving vendors toward best practices can help all boats to rise with the tide, including improvements in the development, testing, and continual evolution of vendors' products.
- **Others who can help secure elections.** This includes the U.S. Election Assistance Commission (EAC), the U.S. Department of Homeland Security (DHS), state chief information officers and chief information security officers, state homeland security advisors, fusion centers, election integrity groups, academics, and other non-profits and private companies willing to lead or support various efforts. This is, in many ways, a baselining effort that we hope supports other efforts dedicated to improving the security of elections, both new and ongoing.
- **Voters, the media, and other interested stakeholders.** In the end, no stakeholder matters more than voters. Not only is it the duty of all to ensure elections represent the will of voters, but it is the duty of all to ensure that voters have confidence in the process before heading to the polls and after results come in.

Goals and outcomes

This handbook is about establishing a consistent, widely agreed-upon set of best practices for the security of systems infrastructure that supports elections. It provides both a general explanation of the threats that exist for the various components of the elections process and examples of known mitigations for these threats.

By developing and publishing this handbook, CIS aims to establish a baseline of protection for all aspects of the elections infrastructure ecosystem that leverage digital tools and applications. The primary goal of this handbook is to impact and improve the security of elections infrastructure as soon as possible, and ideally in advance of the 2018 elections, and establish a set of best practices that, with continual updates, supports elections infrastructure security into the future. We expect many elections systems will already incorporate the majority of these mitigations, allowing those jurisdictions to demonstrate a strong baseline. In that case, the handbook can assist in prioritizing for continual improvement and evolution.

Handbook structure

This handbook is divided into three parts that together provide a baseline view of how to manage cybersecurity risk in elections:

- **Part 1: Introduction.** This introductory section describes this handbook and provides some general information on risk assessments in elections systems.
- **Part 2: Elections Systems and Risk**. The second part **introduces a high-level generic elections architecture,** some components of which may exist at the state level, some at the local level, some both, and some not applicable in certain jurisdictions. It also **classifies these common components of elections systems according to the manner in which they are connected to networks or other systems.** For each major component of the generic elections infrastructure, there is an overview and description of how it fits in the elections landscape and a brief description of the risks and

threats associated with the component. Finally, it summarizes the classification-based ways that different implementations of the components are connected to other digital infrastructure.

- **Part 3:** **Mitigating System Risk.** The third part is a **technical best practice guide that provides controls and recommendations for systems.** It includes two major sections: 1) a set of critical risk-mitigating activities that can benefit any organization and 2) a set of technical best practices for users, devices, software, and processes that are listed first for components that are network connected and then for those that are indirectly connected. We also provide technical best practices that address transmission of information among digital components of the elections infrastructure. As described below, the nature of the connectivity to other elements of the elections digital infrastructure is the major security vulnerability area and thus we have chosen this connectivity as the basis for organizing technical controls. Technical staff, whether government or contracted resources, should be able to implement these controls to provide an appropriate mitigation of risk.

What this handbook is not

A shortcoming of many efforts in domains as large as IT security and elections is a failure to properly scope efforts. In addition to describing what this handbook is, we want to be explicit about what this handbook is not.

Aspects of elections, voting, and protecting democratic institutions that are not part of the scope of this handbook are not an indication of importance, but rather an acknowledgment that no single effort can successfully address everything. This handbook limits its scope to only digital aspects of elections themselves, though in some cases it references paper-based processes in order to further the discussion. The one exception to this is the recognition of how the means of transmission can inject cybersecurity risks, such as digitally transmitting to-be-paper pollbooks to a printer. In these cases, we identify the transmission risks in Part 2 and the mitigations to transmission risks in Part 3.

Beyond this, there are several aspects of election security we do not address. This handbook is <u>not</u>:

- **A one-size-fits-all.** This handbook **does not recommend any single approach to managing election systems or developing and deploying elections systems technology.** Election jurisdictions tailor their voting processes and systems to the needs of their voters and jurisdictional laws and requirements. That said, there are many commonalities. Rather than focus on differences of approach, this handbook focuses on the best practices associated with common approaches, recognizing the variety of approaches and architectures wherever possible.
- **An all-encompassing scope.** As this handbook is about improving the security of elections infrastructure as it exists today, **we have intentionally left several aspects of the broader voting process, however important, out of scope:**
  - Eligibility for an individual to register to vote;
  - Voter identity verification, unless specifically about the accuracy and availability of voter registration rolls;
  - Security of campaigns or campaign information systems; and
  - The accuracy of information about candidates or issues, including those conveyed using social media.

Assessing risk in elections systems

A common way of describing an organization's cybersecurity posture is in terms of risks that have been mitigated and risks that have been accepted. Those outside the information security community will often think of security in terms of stopping all possible threats. Both within the community and in the legal domain, practitioners understand that perfect cybersecurity is not possible. Rather, organizations seek to achieve "reasonable" security that involves accepting some level of risk given the threats and potential consequences, while maintaining an ability to recover should any of those consequences be felt.

Elections systems risk overview

The IT systems infrastructure that supports our elections processes has myriad risks, and these risks vary from one organization to the next. There are a number of commonly used risk assessment approaches that can be used by election officials and their technical staff to help assess risk, such as International Organization for Standardization (ISO/IEC) 27005 and National Institute of Standards and Technology (NIST) Special Publication 800-30. Among the most popular tools for understanding and managing cybersecurity risk is the NIST Cybersecurity Framework, which organizes cybersecurity activities in five functions: identify, protect, detect, respond, and recover.

Unfortunately, many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems.

In its simplest form, a risk assessment is used to identify and assess the impact of vulnerabilities—weaknesses that an attacker can exploit—while being mindful of the compensating controls that exist in a system. These risks can be mitigated with appropriate physical, process, and technical safeguards. In this way, risk and potential impacts can be reduced to a level deemed acceptable by the accountable election officials, often called a balanced risk posture. The potential impact or consequence of a successful exploit is an important part of a risk assessment as elections officials want to focus first on exploits that have the greatest potential consequence. While some risks vary from one election jurisdiction to another, many are common across the wide variety of elections systems configurations. As part of producing this handbook, experts have collaborated to assess the common risks to elections systems. This common baseline risk assessment has influenced the prioritization of security best practices in the handbook.

Baseline elections risk assessment

The baseline assessment of risk for elections is summarized for the purpose of helping election officials and their technical staffs understand the major areas of risk that can serve as their primary focus. Each organization should augment the baseline elections risk assessment to address the risks that might be unique to their elections processes, systems, and threats.

Examples of threats and consequences

Scenario 1:
A nation-state uses the internet to access and disrupt one or more state voter registration databases such that legitimately registered voters are denied the ability to vote on election day, or are required to file a provisional ballot.

Consequence:
Although no votes are manipulated, this attack would likely be a major national news story that results in reduced confidence by the public in the integrity of the voting process and the election results. Additionally, this slows the voting process, creating the risk of long lines and making in-person voting less efficient.

Scenario 2:
An adversary gains access through the internet to one or more election night vote displays and changes the displayed results such that the real winner of the election is now the reported loser in the election.

Consequence:
Again, while no votes have been changed, and the erroneous posting of election results by an authoritative source will subsequently be republished correctly, there is likely to be a significant loss of voter confidence.

A top-level assessment of vulnerabilities and potential consequences to the elections systems infrastructure identifies network connectivity—devices or systems that work with other devices or systems to achieve their objectives—as the major potential vulnerability. The reason is simple: given an adversary with sufficient time and resources, systems that can be accessed via a network cannot be fully protected against compromise. There are ways to improve the security of network connected systems with additional controls, but the inherent complexity of network connectivity results in significant residual vulnerabilities.

Therefore, risks for system components that are connected to a network should be treated differently than for components that are never connected to a network. In this handbook, the definition of "network" includes connections to the internet as well as connections to both local wired and wireless networks.

While systems that are continuously connected to a network have a somewhat higher risk than systems that are only intermittently connected to a network, experts have demonstrated that any network connectivity, even if only for a limited period of time, results in a significantly larger vulnerability profile. An access path to these components may be available through the internet if any connected component can access the internet, and thus an attack can be orchestrated from anywhere in the world. The box to the right illustrates examples of these threats.

On the other hand, systems that have a digital component but are not network connected have a reduced vulnerability profile. Specifically, there are fewer ways to attack such systems and devices, but it does not mean the consequences of a successful attack are any lower—indeed, an attack can still be executed without geographic boundaries. The methods used to upload and download information (e.g., USB sticks, memory cards) still have vulnerabilities, but there are fewer vectors of attack to mitigate.

Three classes of elections systems

In this handbook, we have organized best practices into two classes based on the different threat characteristics associated with levels of connectedness. A third class, that of processes that are executed without a digital component, such as hand-counted paper ballots—the casting and counting of ballots via purely paper and manual means—is out of scope for the handbook.

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. Throughout this handbook, we classify components of elections systems based on three types of connections that most clearly define the risk landscape:

1. **Network connected systems and components.** Network connected components are interconnected with other devices to achieve their objectives. 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. As an example, an Election Management System (EMS) connected to a private county network would still be classified as a network connected system.

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 or other flash media. 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.

3. **Non-digital elections components.** These are aspects of the elections process that have no digital component and are **out of scope for this handbook.** 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 the ballot— may leverage digital infrastructure, the aspect of this process that is purely paper-based is out of scope.

In Part 2 of the handbook, each major component of an election system is briefly described and then placed into one of these classes, providing a method to simplify the risk landscape and assist officials and their technical staff in determining the most effective and efficient approaches to managing risk. In some cases, major components are divided into the primary approaches to executing a process, such as the different approaches to conducting vote capture, each of which is classified individually. This classification analysis becomes the foundational basis for an elections organization selecting the appropriate technical best practices for that component described in Part 3 of the handbook.

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—attack vectors in cybersecurity parlance—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. In Part 3, we also address transmission risks of this nature and the best practices that can mitigate them.

Part 2: **Elections Systems and Risk**

A description of major elections components and their risks.

This part of the handbook provides a generalized elections systems architecture showing each major component of the systems and:

1. A discussion of the risks and threats for each major component,
2. For some components, a description of the different types of deployment in use, and
3. A classification of the component based on how it connects to other devices, and thereby a mapping to controls and recommendations in Part 3 of this handbook.

A generalized elections systems architecture

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. That said, many experts have studied the elections process at length, and there are several fundamental components common to nearly all elections systems.

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. Those accountable for elections infrastructure should understand these basic processes and identify the parts where they have purview. A description of major system components that comprise the elections infrastructure are shown in [FIGURE 1].
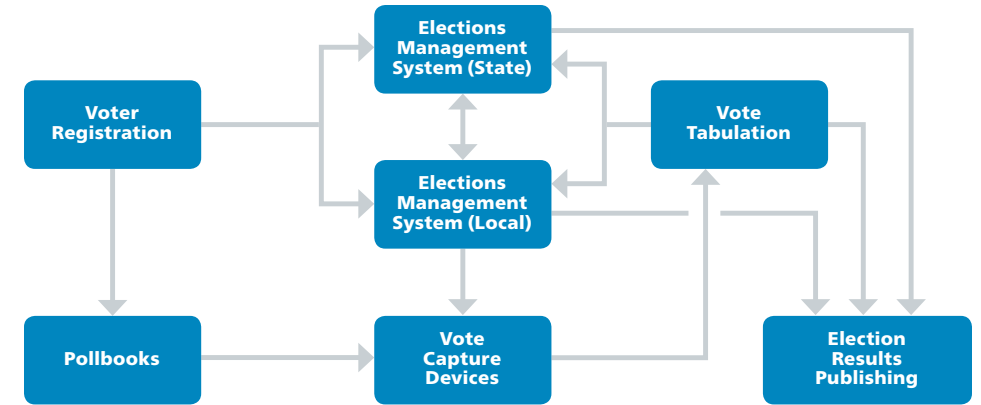

FIGURE 1: *A generalized elections systems architecture*

While each of these systems has IT components that require security best practices, this handbook addresses a subset that are, in our view, the highest risk targets of attack by adversaries and thus require the bulk of the attention. For digital components not covered in the handbook, the analysis methods used here can be applied to determine the appropriate set of technical best practices for that component.

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. Nonetheless, all will exist in most jurisdictions and must be addressed in order to provide a comprehensive best practices guide. This is especially true for local jurisdictions, given the extent to which elections are administered locally. 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 controls are provided in Part 3.

Voter registration

Every state has a unique approach to voter registration—including some states with automatic voter registration—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 a voter), 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.

In all of these cases, there is a master voter database at the state level. The 2014 EAC Statutory Overview describes this database as populated in one of three broad ways:

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 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 and software. 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 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.

[FIGURE 2] shows the major functions or subsystems of a voter registration system.
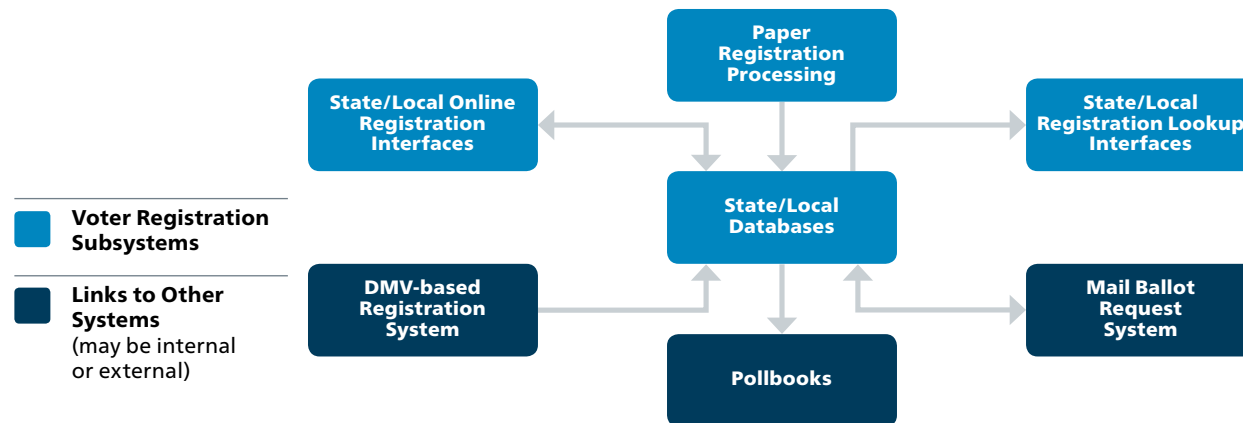
FIGURE 2: *Components of a typical voter registration system*

Types of voter registration

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. Registration of this type is out of scope in this handbook.

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.

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 such as those described in the box to the right, 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 the 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 and software, 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 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.

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. Based on their type of connectedness to digital systems, these controls are listed in Part 3.

In practice: protecting the voter registration database

Cybersecurity practitioners constantly face a difficult balance between convenience for users and strong security. With voter registration databases, some approaches allow elections officials to have it both ways.

Practice #1:
Officials in Washington State leverage what's called a "sneakernet" to move information from an internet-facing copy of the voter registration database and a master version of the database that is not connected to the internet. Officials have to physically move data from one machine to another—usually by moving their sneakers to walk it across the room. This doesn't eliminate all risks, but can help protect sensitive information from attack through internet-based vectors, while still allowing individuals to access their information over the internet.

Officials can only access the database from a special application. This application makes periodic copies of the database in a tightly controlled environment and these copies are used to populate all other interfaces. Similarly, changes to the master database are limited to this application. So updates from, say, the DMV don't directly access the database. They're carefully checked for corruption and moved to the master database through this controlled process.

Practice #2:
Some jurisdictions don't air gap their master voter database but use other methods to balance strong security and real-time election official access to the database. In Colorado, the master database is accessible via networks due to needs such as facilitating same-day registration. Experienced cybersecurity professionals leverage appropriate protections including strong vulnerability and risk management programs coupled with robust access controls, intrusion detection and prevention systems, web application firewalls, and security information and event management integration. Multiple layers of defenses—both computerized and human—are used to sustain operations while minimizing risk.

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 in Part 3 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. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected
1) Online registration.

In addition, the master registration database or system itself should be considered network connected.

Indirectly Connected
N/A

Not connected, out of scope
2) Paper-based registration.

Additional transmission-based risks
Transmission of a registration via email or fax leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3.

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, 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 (e-pollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These e-pollbooks 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 e-pollbooks are typically dedicated software built on COTS hardware and riding on COTS operating systems.

The primary input to e-pollbooks 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, e-pollbooks may require additional inputs and outputs to allow for election day changes.

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.

Risks and threats
Attacks on e-pollbooks 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 e-pollbooks 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 prevents them from casting a ballot or forces them to use the provisional ballot process, but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook.

An e-pollbook 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 e-pollbook 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 e-pollbooks,
- 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 primary risks must be managed to ensure proper management of pollbooks. 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.

How these components connect
Managing risks associated with e-pollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

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, out of scope
Paper-based pollbooks.

Additional transmission-based risks
Transmission of data for paper-based pollbooks for formatting or printing. If this transmission incorporates a digital component, it should incorporate the relevant transmission-based mitigations in Part 3.

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.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware that operate in a networked environment. 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.

Significant consequences may result from successful attacks on an EMS. These potential consequences include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect 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.

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 and whether communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP). Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

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, out of scope
N/A

Additional transmission-based risks
N/A

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 machines or paper ballots. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

To this end, 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 for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a generalized set of recommendations that can 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, as documented throughout this handbook, 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—as well as an activation key (for some electronic machines) and the ballot itself for scanning of a paper ballot. The primary output is, of course, 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 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.

Principles and more through the VVSG

The EAC is currently in the process of developing the Voluntary Voting System Guidelines (VVSG) version 2.0. The draft recommended by NIST and the EAC's Technical Guidelines Development Committee incorporates many of the best practices described within this handbook, such as auditability, access controls, data protection, system integrity, and detection and monitoring. The recommended draft is written as a high-level set of principles and guidelines, allowing specific requirements to change without requiring the full EAC approval process. This provides nimbleness and flexibility in voting systems and their underlying cybersecurity as requirements can be developed and mitigations implemented as threats are identified. More information about the VVSG 2.0 development and proposed draft can be found on the EAC's website.

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.

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 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.*

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 a *DRE device.*

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. When this approach is used, the balloting itself is out of scope as it is via paper means. However, this type of voting can carry transmission-based risks.

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 type of vote capture device we call *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 ballots, election officials must consider especially risks involved in the transmission of the ballot. Whether during distribution or return, if the transmission of the ballot is done via digital means, it is subject to the risks of that transmission mode. In Part 3, there is a set of control measures that provide mitigations for risks in transmission.

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.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

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

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.

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.

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.

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, out of scope

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

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 in Part 3. Aspects definitively executed without a digital component are *not connected, out of scope.*

Vote tabulation

In its broadest definition, vote tabulation is any aggregation or summation of votes. 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. For the purposes of this handbook, 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). Vote tabulation in this handbook is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

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.

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. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

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 no*t network connected,* it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Election results reporting and publishing

After votes are tabulated, results must be communicated both internally and to the public. In any given state, this can take many forms, but, in most cases, the basic process goal remains: getting results as quickly and accurately as possible. This section focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing 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.

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.

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. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, election night reporting will be n*etwork 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, out of scope

N/A

Additional transmission-based risks

N/A

Part 3: **Mitigating System Risk**

Critical activities and best practices in elections infrastructure security.

Mitigating risk is, ultimately, about decisions and actions that establish trust in aspects of a system, leading to confidence in the outcome. Risk must be considered at every stage of a system – requirements, design, development, operation, and even for disposal or retirement (e.g., removal of sensitive information).

Like many systems, for election systems this involves establishing trust in users, devices, software, and processes. Many systems are "composed," or built up from a variety of commercial and purpose-built parts, devices, and software connected via processes and user actions. The results in security decisions about trust are made across many components and brought together at a system level. In other cases, key election system components or services functions are contracted out. This does not change the security responsibility for decision-makers, but forces them to think about how the desired security properties can be specified in contract language and service specifications, rather than implemented directly.

This part of the handbook contains:
1. A set of critical risk-mitigating activities from which all organizations can benefit,
2. Recommendations for best practices in contracting for IT services, and
3. A set of best practices in the form of recommendations and controls for network connected and indirectly connected devices, as well as for transmission of information.

Critical risk-mitigating activities

Auditing
Election officials conduct many audits of all aspects of the election process (e.g., vote by mail processing, training, equipment delivery) and election systems (e.g., voter registration transactions, audit log data). However, the focus of this section is on auditing vote capture and tabulation in an election.

Included in this is to validate that the aggregated results reflect the actual ballots cast. One auditing approach is to select a sample of the ballots and, applying a structured process, do a partial recount of the ballots. This controlled audit is intended to provide confidence that the voting results are accurate based on the results of that partial recount. Moreover, audits provide information to election officials that go beyond the requirements for audit and recounting results; audits are the "production time" opportunity for election officials to know that the systems they are using are working properly.

The approach to auditing can vary based on a number of factors, including requirements that may be established within elections jurisdictions. Some auditing requirements call for a manual recount of a set percentage of ballots, others—including risk limiting audits described below—leverage statistical methods to determine the extent of the recount. Auditing requirements typically also have a trigger for a larger recount or full recount based on the outcome of the initial audit. Given the potential expense of auditing, it is critical to properly design audit procedures to reduce costs while achieving the goals of the audit.

Objective auditing in Linn County

In Iowa, Linn County Election Services hired a cybersecurity firm to conduct an audit of various aspects of the county's elections infrastructure. The firm submitted recommendations, and the county decided which of those to prioritize for implementation. The goal in hiring a third-party vendor was to provide objective, professional advice and assistance. This helps ongoing security efforts and gives confidence to the public that Linn County is taking cybersecurity seriously in its elections.

Almost all states have provisions for a full recount of a contest should the result of that contest fall within the state required recount margin (for instance, many states require a recount for a statewide race if that race is within one half of one percent after certification).

The initial audit size and recount triggers are critically important to a good audit. As important is the method by which the audited ballots are selected. Establishing proper methods for random selection of ballots can have a tremendous impact on the audit's ability to confirm election results or show evidence of tampering.

For election officials, the first step to a good audit is recognizing that records must be kept in order to make an audit possible. This means allocating resources to support an audit, along with procedures for efficiently executing the audit and making it sufficiently transparent for interested parties. While audits are not inherently digitally-based efforts, establishing an audit process, with resources, ballot selection methods, audit size rules, and recount triggers, is a critical aspect of mitigating risk across all aspects of elections.

A best practice: risk limiting audits

A possible weakness in some traditional auditing methods is that often either more ballots or fewer ballots are recounted than necessary to validate the results. This can either produce an audit that doesn't fully validate the outcome of the election, or an audit that is more costly than necessary without increasing confidence in the results.

More recently, the concept of risk limiting audits has been introduced as an approach to auditing election results that is both effective and efficient. In addition to those characteristics necessary in a traditional audit—resources, good ballot selection methods, and prior-determined rules—in a risk limiting audit the size of the audit and recount triggers are based on a "stopping rule" determined by the likelihood that the actual election outcome differs from the reported outcome. Put another way, additional ballots are recounted in the audit until there is a pre-determined statistical

level of confidence that the reported result is correct. As an example, a very large margin of victory will typically result in a relatively small audit size, as a very large error would have to occur to change the outcome. A very close election, on the other hand, would require a larger audit.

In practice: risk limiting audits in Colorado

Recently, the state of Colorado established a legal requirement that all elections be subjected to a risk limiting audit. The Colorado Secretary of State defines the "risk limits" for each election. The risk limits (i.e., the acceptable probability that the election results might not be correct based on the statistical analysis process implemented within the risk limiting audit) will guide the process of selecting the size and distribution of the sample to be subjected to the initial audit, and in turn successive audits if they are required to achieve the risk limit confidence. The trend of leveraging risk limiting audits continues to gain steam, and election organizations should consider Colorado as a use case from which they can learn. The References section of this handbook provides additional information on Colorado's approach.

In a risk limiting audit, the size of the audit is determined by the results of the audit itself. That is, the closer the audited results are to the actual outcome, the sooner the audit ends. This is termed the statistical confidence in an election's results. As soon as a previously-determined confidence threshold is met, the audit can stop. As in all audits, units—precincts, machines, batches of paper records—should be selected using random sampling methods. In a risk-limiting audit, the sample size will depend on the margin of victory and other factors; these other factors may include the number of ballots in each precinct and the overall number of ballots in the contests. In general, smaller margins of victory and fewer total votes cast require auditing a larger percentage of the ballots cast. These methods are well-documented and replicable through sources such as ElectionAudits.org.

Incident response planning

Despite the best efforts of election officials and their technical staff, there is some likelihood that there will be an incident at some point during an election cycle. This is the nature of cybersecurity; the true measure of success is often the resiliency of an organization in the face of these incidents.

Incidents can be minor, having no real potential for impacting the election results or public perception of the elections process, or they could be major incidents requiring prompt action to ensure the actual or perceived integrity of the election results. An incident could be a direct attack on some portion of the election system, or it could be a potential threat that might affect confidence in the system (e.g., a reported major flaw in a foundational COTS component of many election systems).

Experience shows that successful incident response depends almost entirely on planning and preparation—the work done before any incident occurs. Good technical and process controls will minimize the attack surface and also help to enable timely analysis of the incident. Identifying key decision-makers and their roles ahead of time allows for effective response.

Planning and preparing begins with creating a plan for diagnosing and recovering from incidents and exercising this plan. To properly develop and exercise these plans, efforts must include a wide variety of stakeholders—ideally all stakeholders that would be involved in response to and recovery from the incident itself. All stakeholders, including seemingly sovereign ones such as federal, state, and local officials, must collaborate in incident response and recovery; they must also collaborate in preparing for those incidents. As the threats change, so must plans. Officials must update documentation regularly and include specific plans for addressing modern cybersecurity risks, such as those presented throughout Part 2.

In practice: recovery ready in Cook County and California

In Illinois, since 2007, the Cook County Clerk's office has worked with an independent data analysis firm, Data Defenders, LLC, which has implemented its Applied Computer Forensics process, called Election System Auditing (ESA)™, as part of an overall election integrity management plan.

For each election, the forensics process takes three "snapshots" of the election equipment: one prior to pre-election logic and accuracy testing (Pre-LAT), one immediately after Pre-LAT, and a final one after the election has finished and the equipment is returned from the polling places and early voting sites.

These snapshots capture all of the information that makes up the software and firmware. Snapshots are encrypted and hashed so that any tampering with the snapshot will be immediately detectable. The three snapshots' hash values are compared with each to see if the software has been altered at any stage of the election process.

A reference copy of all software and firmware used by the voting system is obtained by the County Clerk from a third party source such as NIST or from a certified

Voting Systems Testing Laboratory. The forensic analysis compares the before and after images listed above to the reference copy and reports on any discrepancies.

The reporting identifies any altered or deleted files, programs, scripts, or other operating components. In the case of a discrepancy, the analysis can recover the information and identify the precise lines of code that were added, altered or deleted.

Not all jurisdictions take this approach. In California, for example, the state requires that a master image be created and that image be reinstalled prior to every election. The master images are created using the trusted build files that are provided to the jurisdiction by the EAC or State of California. The trusted build is the file that is built from the source code that was reviewed and certified.

The decision of how often to create master images are a case-by-case decision, but the broader point remains: the ability to restore from a backup is critical to graceful recovery, and the ability to compare a system to a known good state is critical for identifying problems.

Incident response generally follows a lifecycle of: prepare; detect and analyze; contain, eradicate, and recover; and manage post-incident. Again, it begins with documenting and exercising, but in recovery this includes specific information about the systems and processes that may be impacted, such as knowing the hardware and software comprising specific systems, as well as things such as hashes of critical files—a way to validate whether a file has been tampered with from its last known good state. In preparing for incident recovery, one of the most critical mitigation strategies is to ensure proper backups that are secured separately from the affected systems and networks in advance of a potential incident.

The process of actually recovering starts with understanding the incident. As part of that analysis, decision-makers need to understand the impact of the incident so they can prioritize resources appropriately. Recovery is about getting back to a viable state—in some cases, the priority isn't to directly fix the problem, but rather to work around it to get to the desired outcome without the affected system. This is nothing new in the elections context: when a vote capture device breaks, it may be desirable to fix it, but it may be better at the moment to move to paper ballots so votes can be cast efficiently. The same logic may apply in a cybersecurity context across the elections ecosystem; the most important reaction is often to return to an operational state, even if it's not the optimal state.

Recovery, then, is about getting to the best possible outcome in light of the current circumstances. With proper planning and exercising, officials can avoid the impact of an incident that could prevent successfully executing an election, even when seemingly all has gone wrong.

Attacks such as those that would be directed at an election come with a motivation to impact the election in some way. Nothing serves as a greater disincentive to an attacker than knowing that their target will recover quickly and completely. And little serves to build trust with the public like a plan to achieve an accurate result even if an attack is successful. Just as with other aspects of cybersecurity, by taking the time to prepare before an incident occurs, election officials can actually turn away attackers before they arrive.

Contracting for systems or services

Many organizations use contractors or vendors to provide election system components and services to support elections processes or elections system operations. Election officials should assess the contracted supply chain in addition to support provided internally. In instances where there is contract support, officials should carefully analyze requirements for security and clearly define them in the contract. The government organization that is doing the contracting has the responsibility to assess the security risks for the component or service based on an evaluation of potential threats and security weaknesses or vulnerabilities as well as the probability of occurrence and resulting consequences. Security considerations should be an important consideration in the process of evaluating and selecting a contractor.

If the elections staff is contracting for services that are managed by a contractor or vendor, such as hosting of elections-related software or operations of elections systems, the contract should require that the company providing managed services also provide documentation of their cybersecurity processes and controls, including security metrics that are being collected and monitored. Contractor controls can then be compared to the controls listed in this handbook.

The contract should include a definition of services to be delivered (called a service level agreement or SLA) that includes security controls identified in this handbook. Moreover, a best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits.

For elections system components that are subject to elections system certification requirements, evidence of certification is required. Ideally, there should also be a provision for the contractor to provide security updates to the component over its lifecycle to ensure that vulnerabilities that are discovered are corrected and the component is recertified. For system components or services that are not subject to certification, security requirements will need to align with the particular capabilities or services provided in the contract. Many of the best practices listed in this handbook may be appropriate to include as contract requirements.

In general, the contract should require that the contractor provide a security plan as one of the initial contract deliverables. The security plan should describe how the contractor will meet the security obligations of the contract and specify the security practices and procedures that will be used. Of particular importance in specifying security requirements for contractors will be to address how elections-sensitive information (e.g., ballot layout, voter personal information, vote results) is protected during the execution of the contract and how information records are destroyed.

Additionally, contracts should address the obligations of contracted system operators and public sector clients in regards to identity theft liability, control of and access to public and private data under open records laws, and incident response plans and processes. Where possible, contracts also should specify that vendors transmit network, system, and application logs to the client's security information and event management tools if the client requests. This would allow election officials and their staffs to review and monitor activity instead of being solely reliant on the vendor's capacity for monitoring.

Guidelines for ensuring security of contracted support has been described in the publication ISO/IEC 27002. Specifically, section 15 of the standard describes security issues that should be addressed in dealing with suppliers. The Appendix to this handbook contains a reproduction of this section.

Contracting and technical personnel are encouraged to use this or a similar resource to help identify and assess potential risks as well as responsibilities that will need to be addressed in contract documents and in managing suppliers.

Security best practices

These recommendations are derived from extensive experience understanding the types of vulnerabilities found and attacks experienced across a very wide variety of enterprises, and then translating that into specific and positive steps to mitigate those vulnerabilities and threats. Those recommendations are tailored based on the system and "mission" issues that are unique to elections systems, and the confidence expected for successful outcomes. The process used also examined the various guidelines and specifications used in this sector in order to maintain consistency and minimize overlap.

All of the recommended practices are grouped by class of connectedness (i.e., network connected, indirectly connected, transmission), which was identified as the key factor in assessing security risk. In addition, recommended practices that specifically deal with transmission (electronically or manually) are grouped as a collection for ease of reference.

Network Connected

Network connected components work directly with other devices or systems to achieve their objectives. These connections provide many benefits (e.g., remote diagnostics and management, simple data transfer, rapid updating), but also introduce additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means to accessing and managing the devices, which means organizations must take extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet.

Indirectly Connected

Indirectly connected components are not persistently interconnected with other devices. They do, however, have to exchange information in order to complete their objectives in the election process. While these devices do not carry the same risks associated with being connected to a network or the internet, connecting these components to other devices, either through the use of removable media or direct wired connects, can introduce threats. Mitigating these risks requires a particular set of controls and recommendations when managing the device.

Transmission

In addition to the level of network connectedness, recommendations to address the broader risk of transmission of information across systems are listed separately. These can provide different and sometimes unexpected avenues of attack. These can also involve information transmitted to or from supporting systems that are easy to overlook in terms of security criticality (e.g., the printing of pollbooks, scheduling systems).

Structure of the best practices

Each best practice includes the following information:

- Asset Class (Device, Process, Software, User) — the portion of the overall system to which the practice applies.
- Priority (High, Medium, Low) — from a security perspective (in this handbook, only High and Medium practices have been included).
- Applicable CIS Controls — a cross-reference to the most applicable of the CIS Controls (which can provide a deeper description of this type of practice, and pointers to other information).

We also provide information intended to help decision-makers calibrate the potential challenges of implementation. However, these should be treated as rough guidelines for a "typical" situation – not a rule that can be applied to every election system.

- Potential User Resistance (Yes/No) — Would implementation of the practice be expected to cause resistance or complaints by users and operators of the system? If so, extra care might be needed for rollout or training; and care should be taken so that implementation doesn't encourage the use of risky "work-arounds."
- Upfront Cost (High, Medium, Low) — Does this practice typically require the purchase of new technology, or other significant capital expenditure (High)? Items can be listed as Low when no separate purchase is needed, often because the recommendation can be implemented using existing technology, into the basic configuration of the purchased system, or through operator action.
- Operational Cost (High, Medium, Low) — What are the expected post-purchase costs of this practice? Are there high costs associated with things like supplies (e.g., media, special licensing)?

Summary of connectedness in elections infrastructure components

Part 2 describes the components of a generalized elections system. The end of each subsection classified the different approaches to implementing each component based on the extent to which the component is connected to networks. These connectedness classifications are summarized in Table 1 and form the basis of the best practices. Depending on specific implementation, some of these classifications may vary. However, unless compelling information suggests otherwise, components should be protected at the level indicated.

From Part 2, election officials and others should be able to step through each component to determine the manner (or manners) in which it is implemented in a given election jurisdiction. Once the approach is known, the connectedness classification, summarized here, maps to specific sets of best practices found in the remainder of Part 3.

As noted in Part 2, the components below are a subset that, in our view, reflect the highest risk targets. For digital components not listed below, the analysis methods described in Part 2 can be applied to determine the appropriate correctness class and the associated best practices applicable to that component.

Practitioners can implement these best practices in any order, but we recommend beginning with the high priority best practices.

TABLE 1:
Summary of connectedness for elections infrastructure components

Component		Type within component	Connectedness Class
Voter registration		Master systems and databases	Network connected
	1	Online	Network connected
	2	Paper-based	Not connected
		Transmission of a registration via email or fax	Transmission-based
Pollbooks		e-Pollbook, connects via a wired or wireless network	Network connected
		e-Pollbook, connects via a physical media connection or removable media	Indirectly connected
		Transmission of data for printing via a network connection, website portal, or email	Transmission-based
		Transmission of data for printing via a wired media connection or removable media	Transmission-based
EMS	1	Unless definitively known to have no network capabilities	Network connected
	2	If known definitively to have no network capabilities	Indirectly connected
Vote capture		Vote capture device transmits data for any reason—or if the functionality is enabled regardless of whether it is used	Network connected
	1	Voter marked and hand counted paper balloting	Not connected
	2	Voter marked paper balloting with scanning	Indirectly connected
	3	Electronic voting with paper ballot output	Indirectly connected
	4	Electronic voting with paper record	Indirectly connected
	5	Electronic voting with no paper record	Indirectly connected
	6	Electronic receipt and delivery of ballots conducted remotely	Transmission-based
Vote tabulation	1	Connects via a wired or wireless connection	Network connected
	2	All others	Indirectly connected
Election night reporting	1	If receiving tabulated votes via a wired or wireless connection	Network connected
	2	If receiving tabulated votes via a wired media connection or removable media	Indirectly connected
Election night publishing	1	All	Network connected

Best Practices

The following best practices address the risks identified elsewhere in this handbook. References to resources are listed in the Appendix.

Connectedness Class	Priority
Network Connected	**High**

1 Whitelist which IPs can access the device

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

2 Regularly scan the network to ensure only authorized devices are connected

Applicable CIS Controls

#1.1: Automated Asset Inventory Tool
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

#12.8: Periodically Scan For Back-channel Connections To The Internet
Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
Automated tools should be available to actively scan the internal environment, while DHS and MS-ISAC services can assist organizations with scanning their externally facing assets.

continued:

Connectedness Class
Network Connected

Priority
High

③ Limit the devices that are on the same subnet to only those devices required

Applicable CIS Controls
#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
NIST guidance is available to help the technical team determine how to appropriately segregate assets and permit access to only those devices or systems requiring access: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

④ Only utilize approved and managed USB devices with appropriate device encryption and device authentication

Applicable CIS Controls
#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

continued:

Connectedness Class
Network Connected

Priority
High

⑤ Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials

Applicable CIS Controls
#15.8: Disable Wireless Peripheral Access (Bluetooth, WiFi, radio, microwave, satellite, etc.) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth and WiFi), unless such access is required
and risk acceptance is formally documented.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Microsoft guidance on how to disable Bluetooth: https://technet.microsoft.com/en-us/library/dd252791.aspx.

⑥ Ensure the system is segregated from other independent election systems and non-election supporting systems

Applicable CIS Controls
#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the type of information and the sensitivity of the information processes and stored. Use virtual LANS (VLANS) to protect and isolate information and processing with different protection requirements with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	High	Medium

Resources
While this is an often overlooked control and can require architectural redesigns, this is an important control to pursue. NIST guidance on boundary protection: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

Connectedness Class
Network Connected

Priority
High

---

7 **Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on Internet and extranet DMZ systems**

Applicable CIS Controls
#12.2: Record At Least Packet Header Information On DMZ Networks
On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
The Albert device is part of the MS-ISAC offering: https://www.cisecurity.org/ms-isac/services/albert/. There are a number of commercially-available options, such as: https://securityonion.net/.

---

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)**

Applicable CIS Controls
#15.5: Protect All Wireless Traffic with AES and WPA2
Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
NIST guidance on how to implement secure wireless networks: https://www.nist.gov/publications/guidelines-securing-wireless-local-area-networks-wlans.

---

9 **Use trusted certificates for any publicly-facing website**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Vendor recommendation on deploying certificates with the system. Also, test to verify SSL certificate configuration, with products such as with Qualys: https://www.ssllabs.com/ssltest/.

continued:

Connectedness Class
Network Connected

Priority
High

---

10 Ensure logs are securely archived

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security: https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

---

11 On a regular basis, review logs to identify anomalies or abnormal events

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

---

12 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls
#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft guidance on digital signatures: https://technet.microsoft.com/en-us/library/cc962021.aspx.

---

13 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

continued:

Connectedness Class
Network Connected

Priority
High

14 Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

15 Ensure acceptance testing is done when receiving or installing new/updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

16 Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

continued:

Connectedness Class
Network Connected

Priority
High

---

17 ## Deploy application whitelisting

Applicable CIS Controls
 # 2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Low

Resources
NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

---

18 ## Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards

Applicable CIS Controls
#3.1: Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

#18.7: Use Standard Database Hardening Templates
For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	High	Low

Resources
CIS Benchmarks provide hardened configurations for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/. In addition, NIST provides additional recommendations for baselines https://nvd.nist.gov/800-53/Rev4/control/CM-2. Some vendor products may require tailoring to work with benchmark configured systems. Deviations from the benchmark should be documented.

continued:

Connectedness Class
Network Connected

Priority
High

19 **Regularly run a SCAP-compliant vulnerability scanner**

Applicable CIS Controls
#4.1: Weekly Automated Vulnerability Scanning
Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Medium

Resources
Principal cost beyond the purchase of the tool is the adjudication and remediation of the findings. SCAP validated tools can be found at: https://nvd.nist.gov/scap/validated-tools and there are a number of other commercially available tools.

20 **Utilize EAC certified or equivalent software and hardware products where applicable**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Medium

Resources
Guidance from EAC about their vendor certification process: https://www.eac.gov/voting-equipment/frequently-asked-questions/.

21 **Store secure baseline configuration on hardened offline system and securely deploy baseline configurations**

Applicable CIS Controls
#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Network Connected

Priority
High

---

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.**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

---

23 **Maintain detailed maintenance record of all system components**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST guidance: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

---

24 **Require the use of multi-factor authentication**

Applicable CIS Controls
#5.6: Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

#12.6: Require Two-factor Authentication For Remote Login
Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

#16.11: Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	High	Medium

Resources
Vendor specific. NIST guidance on authentication: https://pages.nist.gov/800-63-3/sp800-63b.html.

continued:

Connectedness Class
Network Connected

Priority
High

---

25 **Require users to use strong passwords (14 character passphrases) if multi-factor authentication is not available**

Applicable CIS Controls
#5.7: User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

#16.12: Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Vendor specific. CIS Benchmarks details how this can be implemented for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/.

---

26 **Limit the number of individuals with administrative access to the platform and remove default credentials**

Applicable CIS Controls
#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Network Connected

Priority
Medium

27 **Ensure that all devices are documented and accounted for throughout their lifecycle**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

28 **Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

29 **Maintain an inventory of assets that should be on the same subnet as the election system component**

Applicable CIS Controls
#1.4: Asset Inventory Accounts For All Devices
Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Network Connected

Priority
Medium

30 **Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

31 **Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Medium	Low

32 **Limit the use of personally identifiable information. When it is required, ensure that it is properly secured and staff with access are properly trained on how to handle it.**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

Resources
Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

33 **Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Network Connected

Priority
Medium

34 **Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities**

Applicable CIS Controls
#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

35 **Implement a change freeze prior to peak election periods for major elections**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

36 **Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

37 **Work with vendors to establish and follow hardening guidance for their applications**

Applicable CIS Controls
#3.1: Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Vendors will typically provide recommendations on how to securely deploy and manage their systems.

Connectedness Class
Network Connected

Priority
Medium

38 **Ensure logging is enabled on the system**

Applicable CIS Controls

#6.2: Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Medium

Resources
Work with Vendor to identify logging capabilities. CIS-CAT can check this configuration item for consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. CIS Benchmarks provides logging recommendations for major platforms: https://www.cisecurity.org/cis-benchmarks/.

39 **Use automated tools to assist in log management and where possible ensure logs are sent to a remote system**

Applicable CIS Controls

#6.6: Deploy A SIEM or Log Analysis Tools For Aggregation And Correlation/Analysis
Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	High	High

Resources
A variety of tools that have various capabilities and costs as well as the effort and rigor of the review and retention of the logs which will have varying costs. Windows Event Subscription Guide: https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

40 **Where feasible, utilize anti-malware software with centralized reporting**

Applicable CIS Controls
 # 8.1: Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
Vendor specific.

41 **Ensure only required ports are open on the system through regular port scans**

Applicable CIS Controls
#9.3: Perform Regular Automated Port Scanning
Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

#9.1: Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Checkable by CIS-CAT and other SCAP-validated tools (https://nvd.nist.gov/scap/validated-tools), and other network scanning tools such as NMAP: https://nmap.org.

continued:

Connectedness Class
Network Connected

Priority
Medium

---

42 **Where feasible, implement host-based firewalls or port filtering tools**

Applicable CIS Controls
#9.2: Leverage Host-based Firewalls
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Medium

Resources
If host-based, can be verified by CIS-CAT: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on implementing firewalls: https://technet.microsoft.com/en-us/library/cc772353(v=ws.10).aspx.

---

43 **Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

---

44 **Ensure vendors distribute software packages and updates using secure protocols**

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Work with the election software vendors.

continued:

Connectedness Class
Network Connected

Priority
Medium

45 **Maintain a chain of custody for all core devices**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

46 **All remote connections to the system will use secure protocols (TLS, IPSEC)**

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as, TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify whether secure protocols are configured consumer grade operating system: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

47 **Users will use unique user IDs**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users:
https://msdn.microsoft.com/en-us/library/cc505882.aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

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.)**

Applicable CIS Controls
#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Low

Resources
For some components this may not be practical to implement.

49 **Ensure that user activity is logged and monitored for abnormal activities**

Applicable CIS Controls
#16.10: Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Medium

Resources
CIS-CAT can identify these at the consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. It is desirable to have a log aggregation or SIEM system in place to aggregate and analyze logs for abnormal behaviors.

continued:

Connectedness Class
Network Connected

Priority
Medium

50 **Regularly review all accounts and disable any account that can't be associated with a process or owner**

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

51 **Establish a process for revoking system access immediately upon termination of employee or contractor**

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Resources on the process potentially involved with termination process NIST: https://nvd.nist.gov/800-53/Rev4/control/PS-4.

continued:

Connectedness Class
Network Connected

Priority
Medium

52 Ensure that user credentials are encrypted or hashed on all platforms

Applicable CIS Controls
#16.14: Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify this configuration on consumer grade operating systems and applications, work with vendor to verify:
https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

53 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls
#16.5: Configure screen locks on systems to limit access to unattended workstations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Work with dedicated purpose election system vendors to verify their products. CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

54 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Connectedness Class	Priority
Indirectly Connected	**High**

55 For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging

Applicable CIS Controls
#13.5: Disable Write Capabilities To USB Devices
If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Medium	Low

Resources
Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

56 Disable wireless peripheral access of devices

Applicable CIS Controls
#15.8: Disable Wireless Peripheral Access (i.e. Bluetooth) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Low	Low

Resources
Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

continued:

Connectedness Class
Indirectly Connected

Priority
High

---

57 **Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC Guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

---

58 **Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

---

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**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

---

60 **Store secure baseline configurations on hardened offline systems and securely deploy baseline configurations**

Applicable CIS Controls
#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Indirectly Connected

Priority
High

61 **Work with the vendor to deploy application whitelisting**

Applicable CIS Controls
#2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	Yes	Medium	Low

Resources
NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

62 **Utilize the most up-to-date and certified version of vendor software**

Applicable CIS Controls
#4.5: Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

#18.1: Use Only Vendor-supported Software
For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low Medium	

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

Connectedness Class
Indirectly Connected

Priority
High

---

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.**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

---

64 **Only use the devices for election related activities**

Applicable CIS Controls
#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Medium	Low

Resources
Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

---

65 **Maintain detailed maintenance records of all system components**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

continued:

Connectedness Class
Indirectly Connected

Priority
High

---

66 ## Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls
#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Indirectly Connected

Priority
Medium

67 ## Utilize tamper evident seals on all external ports that are not required for use

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

---

68 ## Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

---

69 **Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

---

70 **Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

---

71 **Ensure acceptance testing is done when receiving or installing new or updated software or new devices**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

---

72 **Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

73 **Identify and maintain information on network service providers and third-party companies' contacts with a role in supporting election activities**

Applicable CIS Controls
#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

74 **Implement a change freeze prior to peak election periods for major elections**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

75 **Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

76 **Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	Medium	No	Medium	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

---

77 **Ensure the use of unique user IDs**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

---

78 **Ensure individuals are only given access to the devices they need for their job**

Applicable CIS Controls
#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
How to implement least privilege within an organization according to NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-6.

---

79 **Maintain a chain of custody for all core devices**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

---

80 **Ensure all workstations and user accounts are logged off after a period of inactivity**

Applicable CIS Controls
#16.5: Configure screen locks on systems to limit access to unattended workstations

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Work with special purpose election system vendors to verify their products.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

---

81 **Regularly review all authorized individuals and disable any account that can't be associated with a process or owner**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Medium	Medium

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

---

82 **Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Connectedness Class
Transmission

Priority
High

---

83 **Use secure protocols for all remote connections to the system (TLS, IPSEC)**

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that Table5 not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Low	Low

Resources
CIS-CAT can identify whether secure protocols are configured for common operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

Connectedness Class
Transmission

Priority
High

84 **Ensure critical data is encrypted and digitally signed**

Applicable CIS Controls
#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security:
https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Connectedness Class
Transmission

Priority
Medium

85 **Ensure the use of bi-directional authentication to establish trust between the sender and receiver**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Low

86 **For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging**

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their product offerings. Additionally see information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

continued:

Connectedness Class
Transmission

Priority
Medium

---

87 ## Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

---

88 ## Track all hardware assets used for transferring data throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

Appendix:
References and Resources

This section provides references to the resources cited in this handbook, including Section 15 of ISO/IEC 27002, which we reproduce with permission from ISO.

In addition, the website for this handbook, https://www.cisecurity.org/elections-resources/, has additional resources, such as more best practices from local elections officials, that may be useful for readers.

CIS resources

Under the sponsorship of the U.S. Department of Homeland Security, CIS offers a number of services to U.S. State, Local, Tribal, and Territorial (SLTT) government entities at no charge. Specifically, SLTT entities can take advantage of the following resources:

- Become members of the MS-ISAC (Multi-State Information Sharing and Analysis Center) for coordination of cybersecurity readiness and response (https://www.cisecurity.org/ms-isac/)
- Access the CIS Controls—20 foundational and advanced cybersecurity actions that can eliminate the most common attacks (https://www.cisecurity.org/controls/)
- Access the CIS Benchmarks—a set of configuration guidelines to safeguard operating systems, software, and networks (https://www.cisecurity.org/cis-benchmarks/)
- Obtain membership to CIS SecureSuite—a set of integrated cybersecurity resources to help start secure and stay secure (https://www.cisecurity.org/cis-securesuite/)
- Use CIS-CAT Pro, to quickly compare and report on the configuration of systems against CIS Benchmark recommendations (https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/)
- Purchase through CIS CyberMarket—a program to improve cybersecurity through cost-effective group procurement (https://www.cisecurity.org/services/cis-cybermarket/)
- Access CIS WorkBench—a community website that serves as a hub for tech professionals to network, collaborate, discuss technical concepts, and download CIS resources (https://www.cisecurity.org/introducing-cis-workbench/)

CIS has gathered additional resources specific to the elections community at https://www.cisecurity.org/elections-resources/. In addition to an electronic version of the handbook, the site includes additional examples of best practices in use in state and local jurisdictions, as well as other resources that may be useful to organizations implementing the best practices.

CIS also provides support beyond that funded by DHS (called "partner paid" services) if needed by SLTT organizations. Examples of partner paid services include additional Albert sensors and security monitoring services as well as tailored cybersecurity support.

Individuals working for any State, Local, Tribal, or Territorial government should contact CIS at info@msisac.org to find out what's best for their organization. Commercial entities, such as vendors of election systems and service providers, are also welcomed to access many of these services, in many cases free of charge.

Other resources referenced in this handbook

Department of Homeland Security. https://www.dhs.gov/.

Designation of chief State election official, 52 USC 20509 (2014). Accessed at https://www.gpo.gov/fdsys/pkg/USCODE-2014-title52/html/USCODE-2014-title52-subtitleII-chap205-sec20509.htm.

Election Assistance Commission. https://www.eac.gov/.

Election Assistance Commission. (2015). *Election Assistance Commission Statutory Overview: 2014.* Retrieved from https://www.eac.gov/assets/1/1/2014_Statutory_Overview_Final-2015-03-09.pdf.

Financial Sector Information Sharing and Analysis Center. https://fsisac.com/.

Harris, Joseph P. (1934). *Election Administration in the United States.* Brookings Institution Press, Washington D.C. Retrieved from https://www.nist.gov/itl/election-administration-united-states-1934-joseph-p-harris-phd.

International Organization for Standardization. (2011). *Information technology—Security techniques—Information security risk management.* ISO/IEC 27005:2011. Available at https://www.iso.org/standard/56742.html.

International Organization for Standardization. (2013). *Information technology—Security techniques—Code of practice for information security controls.* ISO/IEC 27002:2013. Available at https://www.iso.org/standard/54533.html.

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments.* NIST SP800-30. Available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Available at https://www.nist.gov/cyberframework.

"Principles and Best Practices for Post-Election Audits." Edited by Mark Lindeman et al., Principles and Best Practices for Post-Election Audits, 1 Sept. 2008, www.electionaudits.org/principles.html.

Volunteer Voting System Guidelines, version 1.1. (2015). *Elections Assistance Commission.* Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

Summary of resources referenced in this handbook's best practices

Cisco Systems, Inc. "Configuring IP Access Lists." *Cisco,* 5 June 2017, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

Election Assistance Commission. "Election Management Guidelines." *U.S. Election Assistance Commission (EAC),* https://www.eac.gov/election-officials/election-management-guidelines/.

Fyodor. "Nmap." *Nmap: the Network Mapper - Free Security Scanner,* 1 Aug. 2017, https://nmap.org/.

General Services Administration. "GSA Forms Library." *Basic National Agency Check Criminal History,* 17 Aug. 2017, https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

Johnston, Roger G. "Tamper-Indicating Seals: Practices, Problems, and Standards." *World Customs Organization Security Meeting,* 11 Feb. 2003, http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

Microsoft Corp, Inc. "Digital signatures." *Microsoft TechNet,* https://technet.microsoft.com/en-us/library/cc962021.aspx.

Microsoft Corp, Inc. "Disabling Bluetooth and Infrared Beaming." *Microsoft TechNet,* 9 Feb. 2009, https://technet.microsoft.com/en-us/library/dd252791.aspx.

Microsoft Corp, Inc. "Event Subscriptions." *Windows Server 2008 R2 and Windows Server 2008,* 22 Feb. 2013, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "How to Set Event Log Security Locally or by Using Group Policy." *How to Set Event Log Security Locally or by Using Group Policy,* 7 Jan. 2017, https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Microsoft Corp, Inc. "Lesson 1: Managing User Accounts." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Microsoft Corp, Inc. "Managing Windows Firewall with Advanced Security." *Windows Server 2008 R2 and Windows Server 2008,* 2 July 2012, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "Securing Remote Access." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc875831.aspx.

National Institute of Standards and Technology. (2012). *Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks.* NIST SP 800-153. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-153.pdf.

National Institute of Standards and Technology. (2013). *Special Publication 800-35 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53r4. Available at https://csrc.nist.gov/ publications/detail/sp/800-53/rev-4/final.

National Institute of Standards and Technology. (2015). *Special Publication 800-167: Guide to Application Whitelisting.* NIST SP 800-167. Available at http:// nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

National Institute of Standards and Technology. (2017). *Special Publication 800-63B: Digital Identity Guidelines Authentication and Lifecycle Management.* NIST SP 800-63B. Available at https://pages.nist.gov/800-63-3/sp800-63b. html.

National Institute of Standards and Technology. *National Vulnerability Database.* Available at https://nvd.nist.gov.

Onion Solutions, LLC. "Security Onion." *Security Onion,* https://securityonion. net/.

Qualys, Inc. "SSL Server Test." *SSL Server Test,* (2018), https://www.ssllabs.com/ ssltest/.

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls

15   Supplier relationships
15.1 Information security in supplier relationships
15.1.1 Information security policy for supplier relationships

Control
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance
The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

  a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

  b) a standardised process and lifecycle for managing supplier relationships;

  c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;

e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

g) types of obligations applicable to suppliers to protect the organization's information;

h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;

i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;

k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;

m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information
Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control
All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance
Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

e) rules of acceptable use of information, including unacceptable use if necessary;

f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;

g) information security policies relevant to the specific contract;

h) incident management requirements and procedures (especially notification and collaboration during incident remediation);

i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures; relevant regulations for sub-contracting, including the controls that need to be implemented;

j) relevant agreement partners, including a contact person for information security issues;

k) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

l) right to audit the supplier processes and controls related to the agreement;

m) defect resolution and conflict resolution processes;

n) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

o) supplier's obligations to comply with the organization's security requirements.

Other information
The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers). The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control
Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance
The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain

d) if these products include components purchased from other suppliers;

e) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

f) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside

g) of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

h) obtaining assurance that critical components and their origin can be traced throughout the supply chain; obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

i) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

j) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information
The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication

technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management
15.2.1 Monitoring and review of supplier services

Control
Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance
Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;

b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

f) resolve and manage any identified problems;

g) review information security aspects of the supplier's relationships with its own suppliers;

h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

Implementation guidance
The following aspects should be taken into consideration:

a) changes to supplier agreements;

b) changes made by the organization to implement:
   1) enhancements to the current services offered;
   2) development of any new applications and systems;
   3) modifications or updates of the organization's policies and procedures;
   4) new or changed controls to resolve information security incidents and to improve security;

c) changes in supplier services to implement:
   1) changes and enhancement to networks;
   2) use of new technologies;
   3) adoption of new products or newer versions/releases;
   4) new development tools and environments;
   5) changes to physical location of service facilities;
   6) change of suppliers;
   7) sub-contracting to another supplier.