September 2019
v1.0

CIS Center for Internet Security®

Security Best Practices for Internet-Connected Election Technology

Center for Internet Security®

About CIS

Center for Internet Security, Inc. (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, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. State, Local and Territorial elections offices.

Center for Internet Security®

31 Tech Valley Drive
East Greenbush, New York 12061

T: 518.266.3460
F: 518.266.2085
www.cisecurity.org

Follow us on Twitter @CISecurity

Table of Contents

1 Acknowledgments

Overview

3 Introduction
3 Intended Audience
3 Background and Purpose
5 Document Organization
6 Profile Definitions

Security Best Practices

7 Networking and Architecture
26 Servers and Workstations
39 Software Applications
48 Data
58 Administration

Appendix A:

72 Secure Programming

Appendix B:

82 CIS Controls Descriptions

Acknowledgments

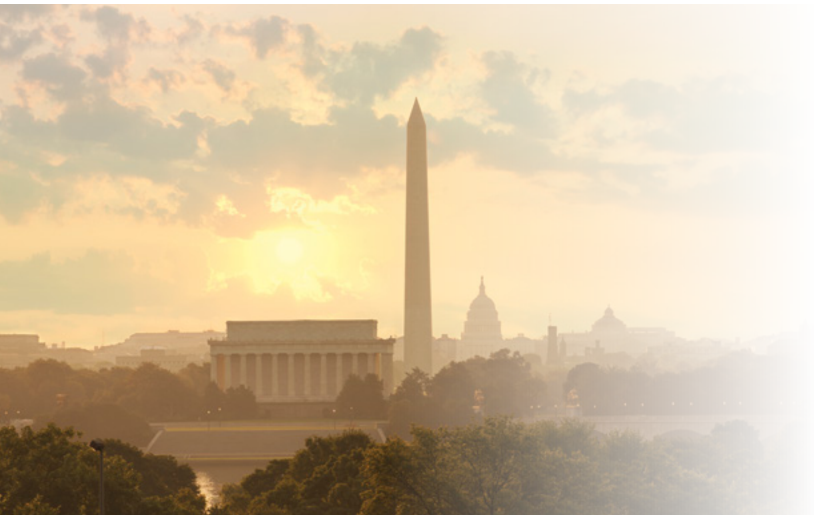
CIS would like to thank state and local election officials, the community of election technology providers, and other stakeholders who volunteered their time and talent to support this important work. CIS products represent the effort of a veritable army of volunteers from across the sector, generously giving their time and talent in the name of a more secure online experience for everyone.

CIS authors and editors

Aaron Wilson

Mike Garcia

Phillip Langlois



Overview

Introduction

The goal of this document is to provide community-driven, comprehensive security best practices and implementation guidance for internet-connected election technology to election officials and election technology providers.

CIS developed this set of best practices for securing internet-connected election technology with a community of state and local election technologists, election technology providers, and other stakeholders. This initiative was built on the set of security controls from the CIS guide titled *A Handbook for Elections Infrastructure Security* to provide specific guidance for securely implementing and deploying internet-connected election technology.

Internet-connected election technology refers to network-connected products and services that handle sensitive ballot, voter, and election results data.[1] This includes election night reporting systems, electronic pollbooks, electronic ballot delivery systems, and voter registration systems.

Election night reporting (ENR) systems receive election results from the voting system and distribute these to various data feeds and host them on a public web application.

Electronic pollbooks (EPB) are used by poll workers to assist with the voter verification and check-in process at a polling location. EPBs typically use the internet to synchronize voter check-ins among all pollbooks.

Electronic ballot delivery (EBD) systems take blank ballot information from the voting system and distribute blank ballots to eligible voters using a web portal.

Other internet-connected voter service applications like online voter registration, polling place lookup, and sample ballot portals are also covered by the best practices in this guide.

These best practices are not intended to secure internet voting systems. Internet voting systems have a very different risk profile and a complex set of unique requirements not covered in this guide.

Intended Audience

This comprehensive set of best practices is intended to be used by technology providers to build and deploy more secure products, as well as help election jurisdictions vet and obtain more secure products. CIS worked with broad group of industry stakeholders to help develop these best practices, including:

- Election technology providers, particularly those who provide election night reporting, electronic pollbooks, and electronic ballot delivery systems.
- Technologists from state and local election offices, particularly those personnel who implement and deploy technology solutions.
- Other government and private organizations involved in the development, implementation, deployment, or monitoring of internet-connected election technology.

Background and Purpose

To enable the free and fair elections that define our democracy, we must protect the security and reliability of election infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand 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.

[1] For the purposes of this document, we use the terms internet-connected and network-connected interchangeably. While not the case in a technical sense, network-connected devices typically share the network with at least one internet-connected device and thus inherit their risks.

Election infrastructure is all the physical, technological, and procedural components required to facilitate free and open elections. Following from the highly decentralized nature of elections in the United States, there is no single catalog of these components nor any agreed-upon way to group them. There are more than 8,000 jurisdictions across the country responsible for the administration of elections. And while the federal government provides some laws and regulations, states have substantial discretion on the process of conducting elections. Moreover, most local election jurisdictions have autonomy to execute elections according to their own customs within the framework permitted by the state.

A Handbook for Elections Infrastructure Security — released by CIS in February 2018 — addressed the totality of election infrastructure. This yielded 88 best practices organized by Connected Class (Network Connected and Indirectly Connected) and Asset Class (Device, Process, Software, and User).

As follow-on work to the Handbook, this guide focuses on a subsection of the overall election infrastructure to provide more specific guidance on internet-connected services. While vote-capture and vote-tabulation devices are not typically connected to the internet, there are several election technologies that are internet-connected. Many of these systems interact with the voting systems or voter registration systems, and some play critical voter-service roles during the election. Due to their connection to the internet, these services are the most at-risk components of the election infrastructure. An attack on one of these services can have significant operational impact on an election, can cause confusion and stress, may potentially disenfranchise legitimate voters, and may ultimately reduce voter confidence in the process. From the perspective of our adversaries, an impact to voter confidence is as good as, or perhaps even better than, an actual disruption to the election infrastructure.

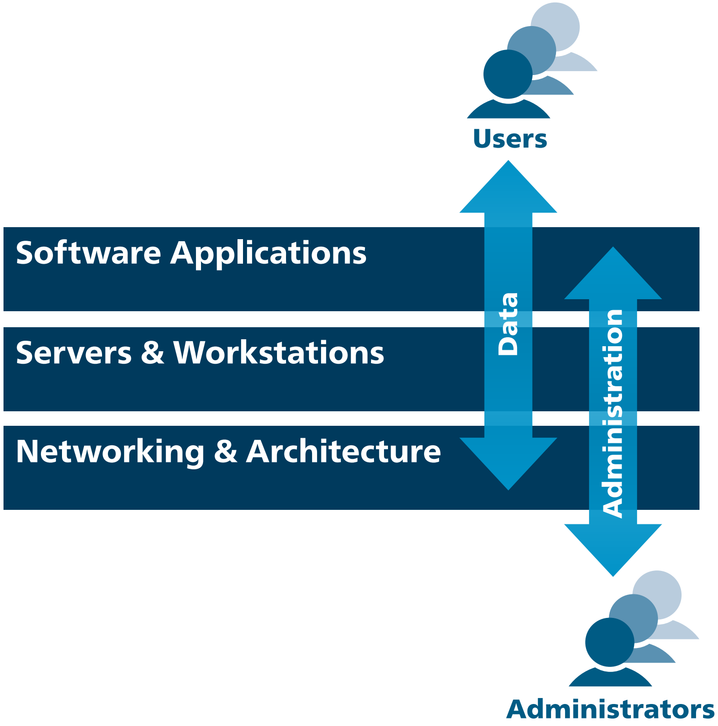
The purpose of this document is to provide a comprehensive set of best practices that, when implemented, will significantly reduce the risk of any of these technologies being compromised and adversely impacting election operations.

The development of the best practices in this guide was governed by the following goals:

- **Risk-based:** The best practices in this guide are recommended and prioritized based on the security risk they are designed to reduce. This helps ensure the best practices that have the highest likelihood of mitigating true threats are prioritized and implemented.
- **Practical and implementable:** The best practices presented are intended to be easily translated into implementable product requirements. We focus on tangible ways to reduce risk that are implementable by most organizations. While we hope this guide sets a bar that technology developers are able to reach, we acknowledge that some organizations will be able to implement some recommendations more readily.
- **Implementation agnostic:** The goal is to elevate the security of all implementations of election technology. To that end, these best practices are written to be implementation and technology agnostic. The intent is for a technology provider to implement these best practices with their current technology in a manner most appropriate for their solution. For some, this may mean they need to update some parts of their products. We can't always prevent that, but there are multiple ways to implement each best practice.
- **Verifiable:** It is important that the best practices be translatable into product requirements for providers, and also translatable into test cases for verification.

Document Organization

This guide is organized into five areas: Networking and Architecture, Servers and Workstations, Software Applications, Data, and Administration. The best practices are grouped into one of these areas. The areas were chosen carefully based on similar threats within each area, and common approach to mitigations and governance. Threats are the types of attacks that malicious attackers are known to perpetrate on target systems. Mitigations are the actions that the system owners and operators take to reduce the likelihood that the threats succeed. Governance refers to the how this area of the election technology stack is typically managed and by whom.



For each area, we introduce the area and provide a discussion on the threats to, and governance of, that area. We then group the mitigations together and provide a discussion on why these mitigations are important for internet-connected election technology. Many of the mitigations are based on the CIS Controls®. For full descriptions of the CIS Controls used, please refer to Appendix B.

The longer narrative texts are designed for nontechnical management personnel who need to understand the rationale and security context. The mitigations are intended for technical audiences who will be implementing the best practices.

Profile Definitions

Each best practice is assigned to one of three profiles. The profiles should be used to prioritize adoption efforts by solution providers with the goal to have all election technology solutions at Level 1 or above. The profiles build upon each other. Achieving Level 2 for a technology solution implies the best practices in both Level 1 and Level 2 are being followed. Level 3 implies that all best practices are implemented.

- **Level 1 –** The Level 1 profile is the set of best practices that are the most broadly applicable and will have the biggest return on investment for most organizations. Some of these may be difficult and costly but, on average, they are the common best practices employed in secure applications and by secure organizations. They address many of the most common threats that an election organization or technology provider can expect to see.

  There may be instances where a Level 1 best practice is not applicable, but these exceptions should be very clear. When an organization deems a best practice as not applicable, it should provide a full justification.

- **Level 2 –** The Level 2 profile provides additional controls for a defense-in-depth strategy for the election technology solution. These best practices will often require more investment in time and resources and greater expertise to implement. Organizations will typically choose which solution components will require deployment of Level 2 best practices.

  We encourage organizations to discriminate between critical and noncritical system components and prioritize deployment of these higher-level best practices on more critical components of the system. Therefore, when deploying Level 2 best practices, two crucial decisions are made that impact the security result: 1) whether to and how to apply the best practice, and 2) to which components to apply the best practice.

- **Level 3 –** The Level 3 profile provides the most advanced and automated security controls. These are the most costly set of controls and must be implemented carefully to avoid any adverse impacts on the functionality of the election technology. As with the Level 2 profile, organizations should implement Level 3 best practices starting with the most critical system components.

Security
Best Practices

1 Networking and Architecture

Networking and system architecture are critical to modern technology. Invisible to most people, modern web-based technology involves behind-the-scenes communication and data storage through networks and on servers around the world. In its simplest view, there are two general architectures: peer-to-peer (P2P) and client/server.

P2P is when one device sends a message directly to another device or devices. These devices communicate over a public or private network. This model has limitations when not all devices are known or available at the time of communication. For this reason, a client/server approach is far more popular.

A client/server allows for many devices to communicate with a persistent central server that maintains the data and can serve it to other devices. Advanced implementations of client/server often involve multiple servers in multiple locations that can serve various types of clients (e.g., mobile apps, browsers) according to their needs. The client/server architecture is the basis for a vast majority of web-enabled products.

There are two common client/server architectures. These are referred to as two-tier and three-tier, referencing the number of places where parts of the technology are implemented. In two-tier architectures, the user interface is stored on the client machine and the database is stored on the server. Database logic and business logic are implemented at either client or server.

In three-tier architectures, the application is split into three parts, namely, the presentation layer (Client Tier), application layer (Business Tier) and database layer (Data Tier). The client system manages the presentation layer, the application server (middle tier) takes care of the application layer, and the server system supervises the database layer. The application layer is used to handle the client request and handle the communication with the database.
The application layer stores all the business logic and data passage logic.

A major architecture aspect is how the system will be hosted. Hosting can be handled by the solution provider, a third party, or the customer. Typically, products that are sold as Software-as-a-Service (SaaS) include the network and hosting management. For hosting done in a data center—hosting outside of a data center is strongly discouraged—there are generally three options.[2]

1. **Co-location –** Company-owned server and network devices are set up in leased space within a data center, typically by renting a server rack that is dedicated to that company for hosting their devices. This approach gives the company full control over the hosting and responsibility for its security and availability.

2. **Managed hosting –** Hardware may be owned or leased by the company, and a third party is responsible for managing the security and availability of the resources. This approach removes some of the control and gives it to a third party, but the company often retains shared control.

3. **Cloud hosting –** Companies pay for hosting as a service and have no ownership over the hardware supporting the hosting environment. The hardware is often shared hardware and the company is purchasing virtualized resources that are dynamically allocated to the company. This has become a popular option.

[2] A data center is a facility that specializes in supporting high-available computing devices such as the servers and network appliances used for web products. Data centers have multiple network and power connections, specialized environmental controls, and robust incident response capabilities.

Each of these models has security strengths and weaknesses. Co-location retains full control of the hosting environment, which means the personnel with privileged access can be fully vetted and there are no restrictions on what security controls the company can put in place. This approach, however, puts a heavy burden on the company to retain expertise in highly specialized areas to keep the infrastructure secure and available. This approach has significant initial expense to the company and is expensive to maintain and scale.

Managed hosting assists with the maintenance demand by outsourcing some of the hosting services but forces the provider to relinquish some control. Managed hosting may be very expensive depending on region and provider. In both co-location and managed hosting, scaling for high peak times and disaster recovery are expensive endeavors. This is why cloud hosting has become a popular option.

With cloud hosting, the underlying infrastructure is abstracted away to provide on-demand services to application providers who don't have the expertise or money to set up and manage a hosting environment themselves. However, since cloud hosting uses shared resources with hidden personnel, it requires handing over significant control of security.

Cloud hosting providers attest to following rigid controls and can usually provide certifications to various international standards. The primary security advantage of cloud service providers is their ability to implement complex and robust security controls that would be prohibitively expensive for many small companies to implement themselves— but it is important to find a cloud provider that meets your security needs upfront and can adjust over time.

The hosting decision comes down to threat prioritization. If the main concern is an attack by a privileged insider, co-location provides the greatest protections. If the main concern is an attack by an external threat, cloud hosting likely provides the greatest protections.

Threats

This section discusses threats that must be addressed at the networking and architecture level.

Distributed Denial of Service (DDoS)

DDoS attacks attempt to overwhelm a resource—such as websites, servers, network devices, or DNS servers—with floods of traffic. Typically, the goal is to slow or crash the system. Flaws in the device software can be exploited to increase traffic and consume resources. Botnets are one growing way that DDoS attacks are executed. Botnets are powerful networks of compromised machines that can be remotely controlled and used to launch attacks of massive scale, sometimes including millions of zombie computers. When used to launch DDoS attacks, they make a target website so busy that it can't process legitimate requests. In fact, DDoS attacks are sometimes able to completely crash the targeted site, and relief may be offered only if the target website owner pays a ransom.

Advanced Persistent Threats (APTs)

APTs are a form of attack where an unauthorized attacker enters an unsuspecting system network and remains there undetected for an extended period. Rather than inflicting damage to these systems, APTs will often quietly attempt to remain on a network undetected, stealing critical information. APTs use various techniques to gain initial access, including malware, exploit kits, and other sophisticated means. APTs typically endeavor to move laterally through networks by scanning and infecting deeper parts of the system or network, inevitably compromising the most valuable and targeted data.

Network Vulnerabilities

Hackers will often exploit vulnerabilities or misconfigurations within network devices to gain unauthorized access to a network. All networks have some sort of parameter with devices and software used to control access to the network. Many of these are charged with permitting some level of access and deciding which access is good and bad. Flaws in the software or hardware running on these devices can be exploited by sophisticated attackers to bypass the security controls designed to make the access control decisions.

Brute Force

Brute force attacks prey on the most common authentication mechanism—username and password. Nearly all components within a network stack will be protected to some extent by a password that may be guessed or "brute forced" by an attacker. The attacker will guess many common password combinations. This technique may be combined with username harvesting. Username harvesting aims to identify legitimate usernames that are often not as well protected as passwords. If the attacker knows legitimate usernames, guessing the password becomes significantly simpler.

Man-in-the-Middle (MITM)

MITM attacks allow the attacker to eavesdrop on communication between two targets, often times relaying messages back and forth without the knowledge of either party. Some of the types of MITM attacks include DNS spoofing, hypertext transfer protocol secure (HTTPS) spoofing, internet protocol (IP) spoofing, address resolution protocol (ARP) spoofing, secure sockets layer (SSL) hijacking, and Wi-Fi hacking.

Insider Threat

Networking and hosting infrastructure is typically managed by a highly privileged set of personnel. Some will have full physical access to the infrastructure while others will have escalated account privileges to the device software. With this level of permission and the typical low level of oversight into these very sensitive and technical devices, these privileged actors have the capability to launch attacks or make unintentional mistakes that can be very impactful. These attacks range from eavesdropping and credential harvesting to full-scale data collection and extraction. Insider threat is not only limited to privileged users, however. Service personnel with access to sensitive areas can be another threat vector.

Governance

Network and hosting infrastructure may be managed differently based on the model used: co-location, managed hosting, or cloud hosting. Since cloud hosting is handled differently than co-location and managed hosting, we separate these into different discussions below.

Co-Location and Managed Hosting

Typically, the hosting and network infrastructure will fall under the technical component of an organization, usually managed by the chief technology officer or chief information officer. The executive responsible will set the policies and manage the risk of the infrastructure to the company and to its users. Underneath this organization, there will be two skill sets. The first skill set is a network engineer or system administrator, who is responsible for managing the network and hosting systems. This technical role includes establishing the configurations and troubleshooting issues. The second skill set is a security analyst, who is responsible for assessing the infrastructure for vulnerabilities and staying abreast of the latest threats and technologies. These two roles work closely together on topics such a secure configurations and patching.

There will be tension between optimizing technology execution and security. In the managed hosting environment, the system administrator and security analyst roles are outsourced to a third party, and the main organization will assign a primary point of contact to coordinate with the managed hosting provider. Making changes in this environment may take time depending on the complexity of the infrastructure. Some changes require very in-depth planning and deployments in phases.

Cloud Hosting

The cloud hosting approach is very different. An organization using the cloud hosting approach creates an account with a provider and a desired level of service. The level of service offered by the provider varies in terms of support level and performance level. The originator of the account will typically become the account holder and can configure the environment according to the settings offered by the cloud hosting provider. This person is typically a technical person who reports to an executive in charge of the hosting and network infrastructure. The options and service available from the provider are typically limited compared to co-location and managed hosting. Changes can be applied more quickly but not all types of changes are permitted. An organization considering a cloud hosting approach must understand their options, especially when selecting which security features to configure.

1.1 Boundary Defense

CIS Control 12: Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Election Technology Application

Boundary defense will apply to all network-connected election systems and their organizations. The first step is understanding what you want as your network boundaries. A network boundary should be created any time there is a different purpose or security paradigm for the devices in the network. At a minimum, every organization with election technology should have two network domains with network boundaries. First, there should be a network boundary established between the internet and your organization's internal network. This allows you to limit the activity from the internet on your own network. Second, network boundaries should separate election systems from both the internet and the organization's network.

This approach is especially important given the public nature of some election technology. Let's first consider election night reporting (ENR) systems. These systems must be exposed to the internet for website traffic. This creates two considerations for boundary defense. First, the network boundary protecting the ENR system from the internet must be robust and well-configured. It must allow only website traffic (ideally only HTTPS) and prevent all other sorts of connections. Second, because you can't limit the origin or the users accessing the site, it is susceptible to many types of attacks, and must be segregated from other networks in case it is compromised. If an attacker is successful in attacking an ENR system, the attacker will have to traverse another robust network boundary before being able to access your internal network and cause more harm.

One technique that is used is to create a network boundary between the servers that serve the webpages and the ones that hold the database. With this approach, the underlying data is protected at a higher level than the server that serves webpages. This approach is preferred for election systems and is critical for voter registration (VR) systems. For VR systems, an additional approach is to completely duplicate the data from the main voter registration database to the system providing online connected voter services such as online voter registration. This enables stricter network boundaries between the primary database and the internet facing systems. In summary, where and how you create boundaries and employ boundary defense mechanisms is extremely important step toward properly protecting your election technology. It is not enough to simply create one boundary between the internet and everything else.

1.1.1 Maintain an Inventory of Network Boundaries

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain an up-to-date inventory of all of the organization's network boundaries.	Deployments of election technology should be segregated into their own network segment. These should be known and kept up to date.	12.1

1.1.2 Scan for Unauthorized Connections Across Trusted Network Boundaries

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections that are accessible across the boundary.	This is one way to tell if there are violations or vulnerabilities in network boundaries. This should be done prior to critical election periods.	12.2

1.1.3 Deny Communications With Known Malicious IP Addresses

Profile Applicability:
Level 1

Description:
Deny communications with known malicious or unused internet IP addresses. Limit access to trusted and necessary IP address ranges at each of the organization's network boundaries.

Notes:
This can be done using a network firewall at the perimeter of your election network. Preventing access from known malicious IP addresses can be done for all election applications, even public-facing ones. The Election Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) provides a list of known malicious IP addresses.

CIS Control:
12.3

1.1.4 Deny Communication Over Unauthorized Ports

Profile Applicability:
Level 1

Description:
Deny communication over unauthorized transmission control protocol (TCP) or user datagram protocol (UDP) ports or application traffic to ensure that only authorized protocols are allowed to cross each of the organization's network boundaries.

Notes:
Election system boundaries should be configured to deny traffic on all ports except ports explicitly needed for legitimate traffic.

CIS Control:
12.4

1.1.5 Configure Monitoring Systems to Record Network Packets

Profile Applicability:
Level 2

Description:
Configure monitoring systems to record network packets passing through each of the organization's network boundaries.

Notes:
This is helpful to detect both vertical and horizontal movement across network domains, especially between a production election technology network and a standard office network.

CIS Control:
12.5

1.1.6 Deploy Network-Based IDS Sensors

Profile Applicability:
Level 1

Description:
Deploy network-based Intrusion Detection System (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

Notes:
The EI-ISAC and the Albert sensors together capture and monitor network traffic of election jurisdictions. Election technology deployed outside of a jurisdiction's network should have a similar technology deployed and monitored.

CIS Control:
12.6

1.1.7 Deploy Network-Based Intrusion Prevention Systems

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Deploy a network-based intrusion prevention system (IPS) to block malicious network traffic at each of the organization's network boundaries.	This should be applied to all network-connected election technology. It must be configured and monitored to ensure it does not prevent legitimate traffic.	12.7

1.1.8 Deploy NetFlow Collection on Networking Boundary Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Enable the collection of NetFlow and logging data on all network boundary devices.	This is performed by the EI-ISAC Albert sensors, if used.	12.8

1.1.9 Deploy Application Layer Filtering Proxy Server

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Ensure that all network traffic to or from the internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	This allows deeper, protocol-specific evaluation of traffic that may be beneficial in protecting the most critical election systems.	12.9

1.1.10 Decrypt Network Traffic at Proxy

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Encrypted traffic can hide cyber threats. The most critical election technology should implement a way to decrypt traffic for analysis by antivirus, advanced threat detection, and data loss prevention systems.	12.10

1.1.11 Require All Remote Access to Use Multifactor Authentication and Encryption

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Require that all remote access to the organization's network and systems use multifactor authentication (MFA) and be encrypted.	Remote access to election technology should be limited to select personnel who are authenticated via MFA over encrypted channels.	12.11

1.1.12 Manage All Devices Remotely Logging Into Internal Network

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	Limit the number of devices that are connected to election technology network segments and keep standard business networks separate.	12.12

1.2 Limitation and Control of Network Ports, Protocols, and Services

CIS Control 9: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Election Technology Application

For all internet-connected election technology, the attack surface should be reduced to the smallest possible area. This will look different for specialized products compared with public-facing solutions. For example, an electronic pollbook solution that uses a hosted database to synchronize voter check-ins between devices can lock down the ports to a single protocol. Other services, such as election night reporting, which serve webpages to the public may need to have additional open ports. Care should be taken to only open the minimum number of ports required to enable the desired functionality.

1.2.1 Associate Active Ports, Services, and Protocols to Asset Inventory

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	It is important to know which ports and protocols each election system needs to perform its function. This may look different for each election system. The list should be documented and kept up to date.	9.1

1.2.2 Ensure Only Approved Ports, Protocols and Services Are Running

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	Election system endpoints should be configured to deny traffic on all ports not explicitly enabled for a valid reason. Each endpoint and port combination should be assessed separately.	9.2

1.2.3 Perform Regular Automated Port Scans

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Regularly perform automated port scans against all systems, and alert if unauthorized ports are detected.	This should be done on a schedule or prior to each election to ensure that only approved configuration changes have occurred.	9.3

1.2.4 Apply Host-Based Firewalls or Port Filtering

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	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.	With many devices, start by applying this to all new devices, then election technology servers, and continue until all endpoints have properly configured host-based firewalls.	9.4

1.2.5 Implement Application Firewalls

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Application firewalls are best placed on the network where the election technology servers share a boundary with the internet.	9.5

1.3 Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

CIS Control 11: Establish, implement, and actively manage (track/report on/correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Election Technology Application

All internet-connected election technology uses network devices to handle and route network traffic. Examples of network devices include IDSs, firewalls, routers, and switches. The security of network devices is critical. Depending on the hosting approach, the solution provider may have to perform this security maintenance task themselves. If so, it is important they maintain a regular process for validating their configurations and patching the devices. Cloud hosting providers will typically handle this maintenance for the solution provider. All election technology should follow these recommendations for securing the network devices involved in handling traffic.

1.3.1 Maintain Standard Security Configurations for Network Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain standard, documented security configuration standards for all authorized network devices.	This is especially important for all network devices that enforce a network boundary between the election solution and another network segment.	11.1

1.3.2 Document Traffic Configuration Rules

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	This is important for production networks that host election solutions. Exceptions are normal but should be few and must be removed when no longer necessary. This is one good reason to keep general purpose workstations in a separate network segment.	11.2

1.3.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.	Secure CIS Benchmarks™ are available from CIS for some network devices. Automated tools are available to CIS SecureSuite® members. All members of the EI-ISAC have access to SecureSuite.	11.3

1.3.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Install the latest stable version of any security-related updates on all network devices.	Ensure that you are monitoring for updates and applying them as you are able. This may require a plan to make updates prior to sensitive election dates.	11.4

1.3.5 Manage Network Devices Using Multifactor Authentication and Encrypted Sessions

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Manage all network devices using MFA and encrypted sessions.	The ability to manage network devices should be limited to authorized personnel accessing the management interface locally or using MFA in encryption sessions.	11.5

1.3.6 Use Dedicated Workstations for All Network Administrative Tasks

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Ensure network engineers use a dedicated machine for all network administrative tasks or tasks requiring elevated access. This machine should be segmented from the organization's primary network and not be allowed internet access. This machine should not be used for email, composing documents, or surfing the internet.	This technique helps ensure the network devices are not introduced to malware that may be trying to infect a sensitive network device.	11.6

1.3.7 Manage Network Infrastructure Through a Dedicated Network

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Some network devices provide a separate management interface. Where available, this separate interface should be used.	11.7

1.4 Data Recovery Capabilities

CIS Control 10: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Election Technology Application

In the event of a security or operational incident during an election, having full system and data backups is key to quick recovery of services for voters. They are critical to recovering from ransomware and other data corruption techniques. Backups are also critical when determining the impact of an attack. The type and frequency of backups may be different for election technology compared with more traditional technology and may vary based on the type of election technology. For example, voter registration data should be backed up on a regular basis throughout the year, whereas electronic pollbooks may need to be backed up at a higher frequency for a short period of time during their use.

Each election jurisdiction should determine its optimal system and data backup strategy. At a minimum, all critical election systems should be backed up prior to each election period after they have been tested and verified by the election authority. Similarly, all critical election data should be backed up nightly during the election period.

In addition to performing regular backups at critical junctions, election officials should regularly test the backup restoration process. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional. In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

Finally, it is important to protect backup data at the same level as production data, especially if the backups contain confidential information such as voter personal information. It is also critical to protect the integrity of the backups to ensure you are reverting to known good data and configuration in the event the backups are used.

1.4.1 Ensure Regular Automated Backups

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that all system data is automatically backed up on a regular basis.	Backups of election data should be done on a nightly basis. There may be applications that need to back up data at even higher frequencies during critical election periods.	10.1

1.4.2 Perform Complete System Backups

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	These types of backups should be done prior to each election for each type of election system used. This allows for quick recovery back to the known good version. Maintaining extra units created from these system backups is another good approach.	10.2

1.4.3 Verify Data on Backup Media

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	This is important to do once per election or more frequently for some systems.	10.3

1.4.4 Protect Backups

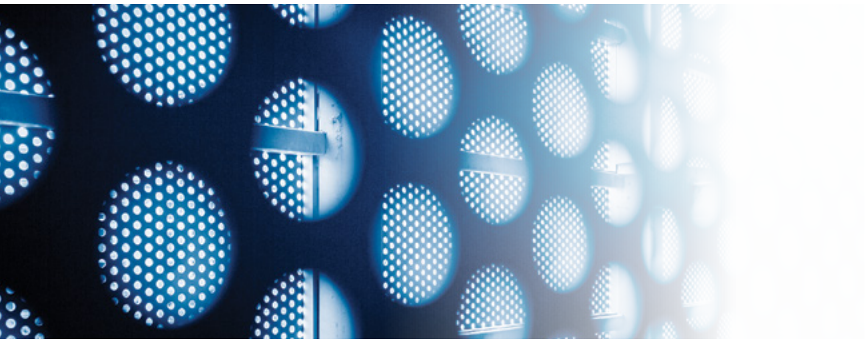
Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes any remote backups and cloud services.	Election data backups may contain sensitive information and are the key to quick recovery. These should always be protected, and access to them should be heavily restricted.	10.4

1.4.5 Ensure All Backups Have at Least One Offline Backup Destination

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	The best way to protect election data backups is to store them on removable media in a physically controlled offline location.	10.5

1.4.6 Verify Complete System Recovery

Profile Applicability:	Description:	Notes:
Level 3	Ensure that all of the organization's key systems are restored from a complete system backup, through processes such as imaging, to verify the quick recovery of an entire system.	Full system recovery should be tested well in advance of each election for each type of election system used. This allows for verification that quick recovery back to the known good version is functioning properly.



1.5 Denial of Service Protections

A denial of service (DoS) or distributed denial of service (DDoS) attack is an attempt to make an online system unavailable to users. This is usually done by temporarily interrupting or suspending the services of its hosting server. A DDoS attack is launched from numerous devices, often distributed globally through what is referred to as a botnet. It is distinct from other DoS attacks that use a single device to flood a target with malicious traffic.

There are three types of denial of service attacks. The first—and most popular—are known as volume-based attacks. These types of attacks include user datagram protocol (UDP) floods, internet control message protocol (ICMP) floods, and other spoofed-packet floods. (UDP and ICMP are protocols in the suite of network protocols commonly used in internet traffic.) The attacker's goal is to saturate the bandwidth of the attacked site with the hope of preventing users from accessing the site.

Second, there are protocol attacks such as SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, and more. This type of attack consumes actual server resources and prevents the system from responding to users.

Finally, there are application layer attacks such as low-and-slow attacks, group encrypted transport/power-on self-test (GET/POST) floods, attacks that target Apache, Windows or OpenBSD vulnerabilities, and more. The goal of these attacks is to crash the web server and render the site unavailable.

There are multiple techniques for executing a denial of service attack. One technique is called Reflection. A Reflection attack occurs when the attackers spoof their IP address to pose as the intended victim and then send legitimate requests to legitimate public-facing services. The responses to these requests are sent to the victim and originate from legitimate servers.

A second technique is called Amplification. Usually used in conjunction with Reflection attacks, Amplification occurs when the response that is sent to the victim is larger than the request that is sent from the attacker. The attacker is able to orchestrate this by requesting a large amount of data from a third-party system. This might occur when the attacker spoofs its IP address, pretending to be the victim, and requests all known data from a public server. This results in the attacker sending a request that is small in size, but results in the public server responding to the victim with a large amount of data.

In addition to the use of botnets, open source tools are freely available online that allow amateur cyber threat actors to perform DDoS attacks. Most of these tools were originally designed to be stress testers. Popular examples of these tools include the Low Orbit Ion Cannon (LOIC) and the High Orbit Ion Cannon (HOIC). These tools can be downloaded, installed, and used by anyone who wishes to be a part of an ongoing DDoS attack. With the goal of consuming all available bandwidth allocated to the target, the LOIC sends significant amounts of transmission control protocol (TCP) and user datagram protocol (UDP) traffic, while the HOIC specifically sends HTTP traffic. Other examples of tools that can be used to perform DDoS activities include Metasploit, Pyloris, and Slowloris.

Election Technology Application

DoS attacks are particularly concerning for applications where availability within a set time period is critical, such as with elections. Election Day and the legally defined time periods identified around it could make DoS attacks very effective at disenfranchising voters and sowing frustration and distrust.

A DoS attack against a service that is only legally available for a short time period can have acutely disastrous consequences. For example, Election Day voting using electronic pollbooks is a service that may only available for 12-15 hours on a preset date, and of those hours there are a few which are known to be higher volume periods. A DoS attack during peak hours would create long lines at polling locations. Some of this may be mitigated with reverting to paper pollbooks and extending polling hours, but voters may still be disenfranchised if they cannot vote at their preferred time with minimal waiting. The same is true of election night reporting. Early voting or in-person absentee voting with electronic pollbooks has a longer time frame, putting the attacker in a position in which a more sustained—and thus more expensive—attack is necessary to have the same impact. Nonetheless, any impact can undermine confidence, achieving at least some of the desired impact.

A number of tactics can be used to mitigate a DoS attack, though none will completely prevent a large-scale distributed denial of service (DDoS) attack during a high-volume period. To best address this risk, election jurisdictions and technology providers should make accommodations for backup plans if a DDoS is waged during a critical time period. For example, electronic pollbooks on Election Day could be designed to run offline and still process voters even in the event a DDoS is waged against the server. Additionally, the jurisdiction could provide paper pollbooks to polling locations as a backup option. For time-critical operations, security layers and redundant options are a must.

One thing that is consistently true about mitigating DDoS attacks is that proper mitigations require planning. Addressing a DDoS attack while it is being executed is extremely difficult if the organization hasn't planned for it. The best practices in this section reflect the criticality of setting up relationships and technical controls ahead of time.

1.5.1 Establish and Maintain Effective Partnerships With Your Upstream Network Service Provider

Profile Applicability:	Description:	Notes:
Level 1	Establish and maintain effective partnerships with your upstream network service provider and know what assistance they may be able to provide you in the event of a DDoS attack. In the case of a DDoS attack, the faster a provider can implement traffic blocks and mitigation strategies, the sooner your services will become available for legitimate users.	Election jurisdictions and technology providers should know and have a relationship with their upstream provider(s). It is important to tell these providers when to expect your periods of critical availability and highest volume.

1.5.2 Port and Packet Size Filtering

Profile Applicability:	Description:	Notes:
Level 1	Consider port and packet size filtering by the upstream network service provider.	Work with upstream providers to filter out as much as possible that is not related to the election service being provided.

1.5.3 Enable Firewall Logging

Profile Applicability:	Description:	Notes:
Level 2	Enable firewall logging of accepted and denied traffic to determine where the DDoS may be originating from.	Most election technology must be careful not to block based on IP address unless there is evidence of malicious behavior.

1.5.4 Configure Perimeter Devices to Prevent Common Types of Attacks

Profile Applicability:	Description:	Notes:
Level 3	Define strict "TCP keepalive" and "maximum connection" on all perimeter devices, such as firewalls and proxy servers. This assists with preventing the success of SYN flood attacks.	A SYN flood is one of the most common forms of DDoS attack observed by the Multi-State Information Sharing & Analysis Center® (MS-ISAC®).

1.5.5 Configure Devices to Detect and Alarm on Traffic Anomalies

Profile Applicability:	Description:	Notes:
Level 2	Configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies. Establish and regularly validate baseline traffic patterns (volume and type) for public-facing websites.	Active and automated monitoring during peak election periods is critical to early detection and mitigation of DDoS attacks.

1.5.6 Establish DDoS Mitigation Services With a Third-Party DDoS Mitigation Provider

Profile Applicability:	Description:	Notes:
Level 3	Consider obtaining third-party DDoS mitigation services.	A number of DDoS protection services have made their offerings available to election jurisdictions. Whether free or at a cost, these services can be very helpful to protect the most critical internet-connected election functions.

1.5.7 Set Up Out-of-Band Communication for DDoS Response

Profile Applicability:	Description:	Notes:
Level 1	Set up out-of-band access, internet, and telephony to an incident management room to ensure connection in the event of a DDoS attack that disrupts normal connectivity.	This is critical to communicate with the public, poll workers, and others during a DDoS attack on election infrastructure.

1.6 Wireless Access Control

CIS Control 15: The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Election Technology Application

Traditional wisdom has been to avoid using wireless technologies in election technology. Certainly, avoiding their use is the lowest risk option. It is possible, however, to use these technologies in some election technologies and mitigate the risk to acceptable levels. Election officials will ultimately determine the level of risk to permit. The goal of these best practices is to provide security measures that will reduce the risk of using wireless technologies when permitted. The important security aspects to cover are device and gateway authentication, encryption of data, and integrity of data.

One important note is that this section is intended to cover the use of wireless technology on devices provided by election technology vendors and used by election jurisdictions. Voters and the public will use wireless technologies to interact with election technology. Their use of wireless technologies is outside the scope of this document.

1.6.1 Maintain an Inventory of Authorized Wireless Access Points

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain an inventory of authorized wireless access points connected to the wired network.	Identify election technology that uses a wireless connection, and document each access point. For Wi-Fi, this will be a Wi-Fi router and any endpoint devices. For Bluetooth and NFC, this may be multiple devices. The decision to enable wireless technology should be made by the election administrator using a risk-based decision-making process.	15.1

1.6.2 Detect Wireless Access Points Connected to the Wired Network

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	This is necessary to alert election technology providers to the presence of unauthorized Wi-Fi access points. For Bluetooth, each device must be checked for whether it has Bluetooth enabled.	15.2

1.6.3 Use a Wireless Intrusion Detection System

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Election technology must ensure there are no unauthorized wireless access points that can be used to access the network. These will become a prime target for attackers looking for a way into the network.	15.3

1.6.4 Disable Wireless Access on Devices if it Is Not Required

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Disable wireless access on devices that do not have a business purpose for wireless access.	Disable all wireless options on election technology devices that are not authorized to use wireless. Periodically review device settings to ensure wireless options (Wi-Fi, Bluetooth, etc.) remain off.	15.4

1.6.5 Limit Wireless Access on Client Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Configure wireless access only on client machines that do not have an essential wireless business purpose. Allow access only to authorized wireless networks, and restrict access to other wireless networks.	All Wi-Fi connected election technology devices must only connect to the authorized wireless access point and no other.	15.5

1.6.6 Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.	If Bluetooth and other peer-to-peer protocols are not actively being used, they should be disabled.	15.6

1.6.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	Wi-Fi, Bluetooth, and NFC all support encrypted communication. Ensure Wi-Fi uses Wi-Fi Protected Access 2 (WPA2) or better. Ensure Bluetooth uses a secure pairing option and requires personal identification numbers (PINs) to authenticate devices.	15.7

1.6.8 Use Wireless Authentication Protocols That Require Mutual, Multifactor Authentication

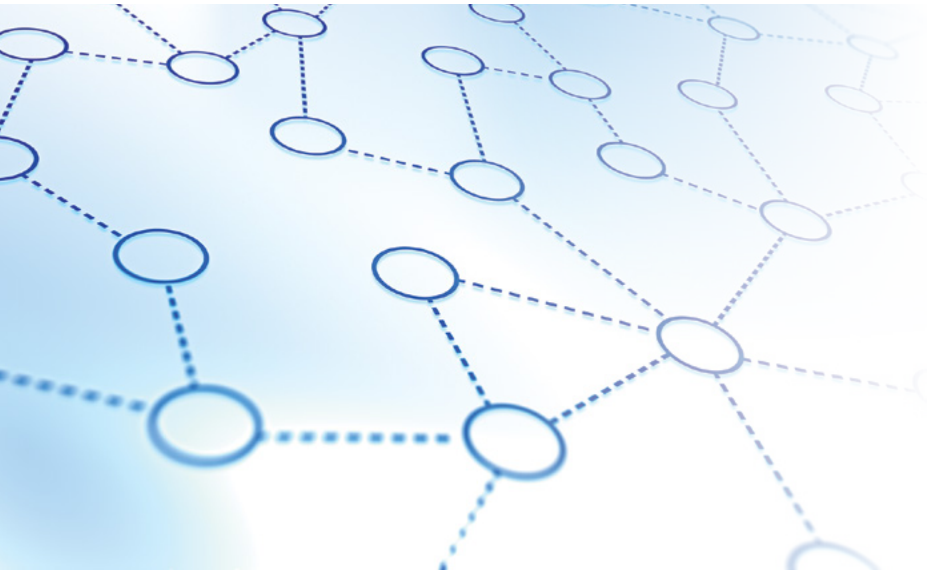
Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual, multifactor authentication.	Use of wireless technology in election technology demands that all parties be properly and fully authenticated.	15.8

1.6.9 Disable Wireless Peripheral Access to Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Printers and other peripherals often have Bluetooth capabilities that should be disabled unless absolutely necessary.	15.9

1.6.10 Dedicated Wireless Networks

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Create a separate wireless network for each separate use. Access from the wireless network should be treated as untrusted and filtered and audited accordingly.	Use of any wireless technology in election technology should be isolated for a very specific purpose, and incoming connections from the wireless network should be handled with care.	15.10



2 Servers and Workstations

Servers and workstations are the devices that provide services to end users or to other devices. These are also referred to as endpoints. Endpoints are typically networked together and often run distributed applications to create a seamless solution across physical boundaries and multiple users. The networking aspects are covered in the Networking and Architecture section of this guide. The software solution is covered in the Software Applications section. This section is focused on the technology that operates on these devices and interacts with the network and supports the application. In most cases, this is the hardware, firmware, and operating system resident on the devices.

Most people think of endpoint security as operating system security. Firmware typically provides a standardized operating interface to the hardware for the more complex software such as the operating systems to use. The operating system manages and oversees the creation of the instructions that are interpreted by drivers and firmware. Operating systems manage which services are running and what permissions those services are afforded. The operating system also manages memory allocation and attempts to ensure programs only work within that allocation. Operating systems also manage users and enforce user authentication and authorization.

In most modern computing, hardware and firmware are very general, commercially available options that provide common computing capabilities and hand over control of those capabilities to the operating system or higher-level programs. In some cases, such as embedded systems, both the hardware and firmware may be customized to provide specific capabilities for a specialized operation. This is becoming less common.

Servers and workstations are not always physical devices. Many endpoints in modern computing are virtualized to make more efficient use of significant increases in hardware capabilities and performance. This also makes it possible to move endpoints around, scale them, and recover them much easier than before. Virtualization has become so advanced it is often impossible to detect whether you are interacting with a virtualized endpoint or a traditional hardware deployment. Nearly all cloud hosting options take advantage of significant levels of endpoint virtualization. Virtualization offers many benefits for computing but the abstraction away from physical devices creates new security concerns.

Threats

The following are the common threats to servers and workstations that should be addressed with adequate mitigations to reduce risk to acceptable levels.

Malware

Malware is malicious software or software designed to perform malicious actions on a device. It can be introduced to a system in various forms, such as emails or malicious websites. Additionally, various kinds of malware have distinct capabilities dependent on their intended purpose, such as disclosing confidential information, altering data in a system, providing remote access to a system, issuing commands to a system, or destroying files or systems. The most prolific types of malware currently include:

- **Spyware** is malware that records keystrokes, listens in via computer microphones, accesses webcams, or takes screenshots and sends the information to a malicious actor. This type may give actors access to usernames, passwords, any other sensitive information entered using the keyboard or visible on the monitor, and potentially information viewable through the webcam. Keyloggers, which mainly record keystrokes, are the most common type of spyware, and ZeuS, the most famous keylogger, has been on the MS-ISAC's Top 10 Malware list for several years.
- **Trojans** (a.k.a. Trojan Horses) are malware that appears to be legitimate applications or software that can be installed. Trojans can provide an attacker full access to the device, allowing the attacker to steal banking and sensitive information, or download additional malware, like Emotet.

- **Ransomware** is malware that blocks access to a system, device, or file until a ransom is paid. Malicious actors use ransomware to either encrypt files (crypto ransomware), erase files (wiper ransomware), or lock systems (locker ransomware) on an infected system or device. Ransomware holds infected systems or files hostage until the victim pays the ransom demand. However, paying the ransom does not guarantee that access to the files will be restored.
- **Click fraud** is malware that uses the target system to generate fake automatic clicks to ad-laden websites. These ads create revenue when clicked on. Kovter, one of the more prolific versions of click fraud, has been on the MS-ISAC's Top 10 Malware list for the past year.
- **Cryptocurrency mining malware (i.e., cryptojacking)** is malware that primarily utilizes a compromised system's resources in order to generate cryptocurrency revenue such as Bitcoin, Litecoin, Ether, or Monero. Cryptocurrency mining malware, like Coinminer, has increased in use over the past year to become one of the more prolific malware variants.

The following are the methods used to infect target systems with malware:

- **Dropped –** Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor.
- **Malspam –** Unsolicited emails, which either direct users to download malware from malicious websites or trick the user into opening malware through an attachment.
- **Network –** Malware introduced through the abuse of legitimate network protocols or tools, such as SMB or remote PowerShell.
- **Malvertisement –** Malware introduced through malicious advertisements. Shlayer, a MacOS trojan, is the first malware since March 2018 to rely on this vector within the Top 10 Malware list.
- **Multiple –** Refers to malware that can currently use at least two vectors.

Remote Execution

Remote code execution is the ability of an attacker to access a device and run executable commands, no matter where the device is geographically located. Vulnerabilities can provide an attacker with the ability to execute malicious code and take complete control of an affected system with the privileges of the user running the application. After gaining access, attackers will often attempt to elevate their privileges. The best way to protect a computer from a remote code execution vulnerability is to fix vulnerabilities that allow an attacker to gain access. Remote code execution is the most common threat posed by the presence of software vulnerabilities. In 2019, Code Execution was the most prevalent type of vulnerability added to the Common Vulnerability and Exposures (CVE) database.

Privilege Escalation

Privilege escalation attacks allow someone with user credentials to access information or capabilities of a higher-level user. It is often accomplished by exploiting a vulnerability, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. There are two types of privilege escalation. Vertical escalation allows the user or process to obtain a higher level of access than the system designer intended. Horizontal escalation allows the user or process to gain access to resources that are outside of the user's context. For example, a voter accessing a ballot of another voter is an example of horizontal escalation. A voter obtaining administrator privileges is vertical escalation.

Governance

Servers and workstations are managed by a variety of users within the election administration context.

Election Technology Servers – These are the primary computing devices that power the election technology, and are often hosted in a data center and managed by skilled personnel. They are the most critical devices to election operations and must be protected with a commensurate level of security controls. These devices are often considered trusted in the security model. Some servers are segregated into a special network zone called the demilitarized zone (DMZ). This is the zone most exposed to the internet and thus most susceptible to remote attacks. Servers in the DMZ are treated with a lower level of trust. The election technology provider is primarily responsible for these endpoints.

Election Technology Workstations – These devices interact with the election technology servers, and may be desktops, laptops, tablets, or phones. They are most often in control of the election technology provider or the election jurisdiction and may be dedicated or standard workstations. These workstations are the most difficult devices to manage and are often used by less skilled individuals. For these devices, central device management can be very helpful to keep track of the devices and enforce consistent protections across a large suite of heterogeneous devices. These devices can be managed by the election technology provider or election jurisdiction personnel.

Voter/Public Workstations – These devices are owned and managed by voters and members of the public who interact with the election technology, and are completely outside of the control of the election jurisdiction and the technology provider. They may be knowingly or unknowingly infected with malware and may be used to attack the election technology. The election technology servers that interact with these workstations must interact only to the extent necessary to provide public services. All voter/public workstations must be treated as untrusted and assumed to have malware on them.

2.1 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CIS Control 5: Establish, implement, and actively manage (track/report on/correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Election Technology Application

Rather than start from scratch developing a security baseline for each software system, election technology providers should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Excellent resources include:

- **The CIS Benchmarks™ Program**
  (www.cisecurity.org)
- **The National Institute of Standards and Technology (NIST) National Checklist Program**
  (https://nvd.nist.gov/ncp/repository)

Many of the CIS Benchmarks come pre-configured on cloud hosting platforms. Election technology providers can augment or adjust these baselines to satisfy local requirements, but deviations and rationale should be thoroughly documented to facilitate later reviews or audits. For more complex implementations, a single security baseline configuration (for example, a single installation image for all workstations) is sometimes not practical. You may need to support different standardized images, based on the hardening necessary to address risks and support the functionality of the intended deployment (for example, a web server in the DMZ versus an application server in the internal network). The number of variations should be minimized in order to better understand and manage the security properties of each.

To manage many devices, commercial and free configuration management tools can be employed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Typical configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems by remotely logging into each managed machine using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

2.1.1 Establish Secure Configurations

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain documented, standard security configuration standards for all authorized operating systems and software.	Using a vetted configuration standard, identify each component of the election technology and choose a secure configuration standard.	5.1

2.1.2 Maintain Secure Images

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain secure images or templates for all components based on the selected configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	This allows rapid and reliable deployment of election technology components.	5.2

2.1.3 Securely Store Master Images

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	It is critical that images used to deploy new components or reimage current components are unmodified from their known good state. Some images will be election-specific and must be created and securely stored prior to the election.	5.3

2.1.4 Implement Automated Configuration Monitoring Systems

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	This prevents accidental misconfiguration and allows election technology providers the ability to prove the component has been properly and securely configured.	5.5

2.1.5 Deploy System Configuration Management Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	Where possible, each component should be inspected and updated with the latest known good secure configuration prior to use in any election.	5.4

2.2 Continuous Vulnerability Management

CIS Control 3: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Election Technology Application

Adversaries will be aware that some election technology is not maintained at the latest patch levels. To mitigate risks associated with this, election technology providers must find other approaches to manage known vulnerabilities. At times, operational concerns about patching during critical election periods will outweigh the desire to apply the latest available patch. At other times, it will be worth the risk to apply patches during critical election periods. Election authorities must be aware of and carefully weigh the tradeoffs of these risks.

Continuous vulnerability management can minimize the frequency of this occurring. Effective vulnerability management links vulnerability scanners with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management. The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month. As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan and set policy for the maximum time allowed before a critical patch is applied.

Finally, it is important to ensure that the vulnerability patching process is a vetted process using known-good suppliers of patches. The rush to patch vulnerabilities can leave a blind spot to a malicious actor who is attempting to introduce malware through security patches. To combat this, make sure that all patches are provided by the original manufacturer wherever possible or a vetted and approved third party. It is always a good idea to rescan for vulnerabilities after applying patches to ensure there are no regression or unintended consequences.

2.2.1 Run Automated Vulnerability Scanning Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Use an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify known vulnerabilities on the organization's systems.	It is important to ensure election systems are scanned prior to, during, and after use in an election.	3.1

2.2.2 Perform Authenticated Vulnerability Scanning

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	These scans provide greater insight into the election system's potential vulnerabilities, especially if the attacker is able to gain some level of privileges into the system.	3.2

2.2.3 Protect Dedicated Assessment Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Use a dedicated account for authenticated vulnerability scans that is not used for any other administrative activities and is tied to specific machines at specific IP addresses.	Ensure that only limited personnel are given credentials to this dedicated account. Consider deactivating the account between scans.	3.3

2.2.4 Deploy Automated Operating System Patch Management Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Deploy automated software update tools to ensure that the operating systems are running the most recent security updates provided by the software vendor.	Ensure all systems are updated until it is no longer appropriate to make changes to a system before an election. Beyond this point, patches should be reviewed by security personnel and a decision should be made on whether the operational risk of patching is greater than the security risk posed by the vulnerability.	3.4

2.2.5 Deploy Automated Software Patch Management Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Deploy automated software update tools to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	Ensure that software is patched until it is no longer appropriate to make changes to software prior to an election. After this date, manually review patches to determine if the operational risk of patching is greater than the security risk of the vulnerability the patch fixes.	3.5

2.2.6 Compare Back-to-Back Vulnerability Scans

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	There should be a full history of vulnerability scans for election systems; tracking progress should show timely closing of vulnerabilities and highlight any regressions.	3.6

2.2.7 Utilize a Risk-Rating Process

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	Election system owners should track vulnerabilities based on the level of risk they pose and prioritize them for remediation. Remediation efforts should be executed year-round and especially prior to sensitive election dates.	3.7

2.3 Malware Defenses

CIS Control 8: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Election Technology Application

Election systems and networks running vulnerable services are likely to be impacted by malware, as it is among the most common malicious activity observed. Certain types of malware, such as spyware, click fraud, and cryptocurrency miners continually run in the background and are likely to drain system resources and slow down all affected systems, reducing the lifespan of systems. Furthermore, spyware, trojans, and ransomware can exfiltrate sensitive data such as user credentials or voter information. Ransomware may also block access to the infected system and data, rendering it useless until it is remediated, or the ransom is paid, and the applicable decryption keys are provided.

In addition to direct impacts, IP addresses or email addresses associated with an infected system may be placed on a blacklist if the malware is trying to connect to other systems. Blacklists are reputation-based lists that cybersecurity professionals use to prevent connectivity with malicious IP and email addresses. Being on a blacklist means that electronic traffic, including emails from and legitimate traffic to and from an election office, may be blocked.

Election officials and technology providers should ensure their organization routinely patches all systems and maintains up-to-date anti-malware protection, like antivirus and firewalls, as these will mitigate most malware. Additionally, election technology providers should maintain up-to-date data backups, which are stored offline, regularly tested for completeness, and provide the ability to reinstall in the event of an infection.

Lastly, election technology providers should prioritize training to help employees recognize malicious emails, as they are one of the most popular vectors of spreading malware. Training should emphasize that employees not open suspicious emails, click links contained in such emails, or post sensitive information online, and never provide usernames, passwords, or personal information to any unsolicited request. After training employees, conduct organized phishing exercises to test and reinforce the concepts using services such as those provided by CIS or through the Department of Homeland Security (DHS) Phishing Campaign Assessment.

2.3.1 Utilize Centrally Managed Anti-Malware Software

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	All endpoints in an election technology solution must use properly installed and constantly running anti-malware software. Central management allows administrators to enforce this rule.	8.1

2.3.2 Ensure Anti-Malware Software and Signatures Are Updated

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	Ensure that all anti-malware instances are receiving signature updates. This requires periodic review of devices within the election technology system.	8.2

2.3.3 Enable Operating System Anti-Exploitation Features and Deploy Anti-Exploit Technologies

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system, or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	This should be considered for election technology servers and other sensitive endpoints.	8.3

2.3.4 Centralize Anti-Malware Logging

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	This assists in the early detection of an incident and ensures the proper security personnel are alerted to malware on the network.	8.6

2.3.5 Enable DNS Query Logging

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	This is used to detect attempts to reach known malicious sites from within your network. This will help detect malware and prevent it from communicating with its command and control infrastructure.	8.7

2.3.6 Enable Command-Line Audit Logging

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Enable command-line audit logging for command shells, such as Microsoft® Powershell® and Bash.	A large percentage of malware uses Powershell and Bash. This logging will assist in the detection of malware and a better understanding of its impact.	8.8

2.3.7 Deploy a Host-based Intrusion Detection System

Profile Applicability:	Description:	Notes:
Level 3	Deploying a host-based intrusion detection system can detect and alarm when protected files are manipulated.	This practice can be used to protect critical election technology assets and ensure the integrity of the operating system programs is protected.

2.4 Controlled Use of Administrative Privileges

CIS Control 4: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Election Technology Application

To prevent the misuse of administrative privileges inside an election technology solution, election administrators and technology providers should deploy the principle of least privilege. This principle demands that each user be given only the permissions necessary to perform their job and no more. When done properly, very few users have administrator privileges. Part of using this solution, of course, means that the technology provides robust access control options, such as supporting role-based access controls, to allow election administrators the ability to assign granular permissions to users. Since elections are run very differently across the nation, a flexible access control model is necessary to allow election officials to follow the principle of least privilege without having to assign all users as administrators. Fortunately, most endpoint software—operating systems, etc.—have robust access control options.

In addition to using the principle of least privilege, administrator accounts should never use default or weak passwords. Many systems come with default passwords. These must be changed. In some cases, passwords are shared among users. Passwords should never be shared among users, and whenever a password must be shared due to system limitations (e.g., an older system allows for only one set of login credentials), it must be changed after each election. Finally, it is critical that administrator accounts and any accounts accessing sensitive information are configured to require MFA.

2.4.1 Maintain Inventory of Administrative Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Knowing who is an administrator on each election technology system is an important step in ensuring you have established the right access controls.	4.1

2.4.2 Change Default Passwords

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	It is critical that default passwords are changed on all election technology components. Change passwords between elections, especially if the password was shared for any reason.	4.2

2.4.3 Ensure the Use of Dedicated Administrative Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and day-to-day activities.	Administrator accounts on election technology endpoints should not be used for anything but administrator level activities and only when necessary.	4.3

2.4.4 Use Unique Passwords

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Administrator accounts must use strong passwords that are unique to that system.	Election technology system administrators should use passwords that are not used for their personal or any non-administrator accounts.	4.4

2.4.5 Use Multifactor Authentication for All Administrative Access

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Use MFA via encrypted channels for all administrative account access.	Election technology administrative accounts have tremendous capabilities to do harm if taken over through a social engineering or other attack. Protecting them with MFA is extremely important.	4.5

2.4.6 Use Dedicated Workstations for All Administrative Tasks

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed internet access. This machine will not be used for reading email, composing documents, or browsing the internet.	Some key election technology administrative tasks are sensitive enough to be performed on an isolated and dedicated computer. This limits the chance of that sensitive task or administrative account being compromised.	4.6

2.4.7 Limit Access to Scripting Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Limit access to scripting tools (such as Microsoft® PowerShell® and Python) to only administrative or development users with the need to access those capabilities.	Election technology may make use of these technologies, but access to them should be limited to only the most trusted and protected accounts.	4.7

2.4.8 Log and Alert on Changes to Administrative Group Membership

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Changes to election technology administrator accounts must be logged and alerted. Quick notification allows for timely remediation in the event of privilege escalation or other attack.	4.8

2.4.9 Log and Alert on Unsuccessful Administrative Account Login

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	This enables election technology administrators to detect attempts to brute force or socially engineer access to administrator accounts.	4.9

2.5 Handling Removable Media

Removable media is useful for moving data between systems, particularly between systems that are not connected to a network. It can also be useful to move large amounts of data. Some instances also use removable media for bootable live operating systems and for bootable installation media. Unfortunately, removable media can also be an attack vector used to silently infect devices it is plugged into. It is not always obvious when a device is infected with malicious code, as there are sophisticated ways of hiding malicious code on these devices. The result is that it is risky to use such media if the source cannot be identified, if the media has been used repeatedly, or if the media has been used on untrusted systems.

USB-based removable media is by far the most dangerous removable media to use. The structure of most USB devices allows them to be converted to provide hidden storage compartments, for the removal of stolen data, for example. USB devices appeal to attackers targeting computer networks that are not connected to the internet—such as those powering critical national infrastructure. The most famous example of this is probably the Stuxnet campaign. In 2009 and 2010, the Stuxnet worm leveraged USB devices to traverse segregated networks and target Iran's nuclear facilities in order to disrupt operations.

Rewritable CDs, DVDs, and Blu-ray Discs are all capable of delivering a malicious payload if auto-run is enabled on a computer.

Election Technology Application

The election technology focused on in this guide is all connected to the internet, and typically communicates with secure offline systems as well. This makes the use of removable media between the internet-connected election technology and voting systems a prime target for attackers. It is also common to move data via removable media between devices on different network segments, which may introduce a way for an attacker to avoid typical network boundary protections.

Electronic ballot delivery systems and election night reporting systems will often communicate with voting systems. Voting systems are regarded as trusted, high-integrity systems. This means the primary concern is with data going into these systems from an untrusted environment. Fortunately, the use cases for electronic ballot delivery and election night reporting systems only involve moving data from the trusted environment (i.e., voting system) to the untrusted environment. The reverse, movement of data from untrusted to trusted environments, should be avoided whenever possible. To accomplish this, it is critical that the removable media used is a new, clean device or has been completely wiped from any prior use. We recommend write-once media whenever possible.

Electronic pollbooks and voter registration systems will often communicate voter information back and forth. Electronic pollbooks have often been exposed to a riskier environment and the voter registration systems are typically in a very locked-down network segment. USB devices can be used to communicate between the two, but this will circumvent any well-designed network boundary controls, creating a new set of risks. If possible, allow the communication to go through these network boundary controls to ensure the data is properly vetted and USB based threats are not introduced. If you use USB devices to transfer data, be sure to follow the best practices in this section.

2.5.1 Establish USB Handling Policy

Profile Applicability:	Description:	Notes:
Level 1	Define the appropriate uses for removable USB media and provide training for employees.	Define which steps in the election process will use USB devices and ensure the appropriate steps are documented for procuring, loading data onto, using, and cleaning USB devices.

2.5.2 Only Procure USB Devices From Reputable Sources

Profile Applicability:	Description:	Notes:
Level 1	Ensure that removable USB media is obtained from a known good supply chain and discard any USB devices that are from an unknown source.	Vet the manufacturer of the USB stick, and do not purchase from any source that cannot be verified, regardless of the price.

2.5.3 Configure Devices to Not Auto-Run Content

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Configure devices to not auto-run content from removable media.	This helps ensure an attacker cannot insert a malicious device and execute it without having user credentials.	8.5

2.5.4 Use Write-Once or Formatted Media

Profile Applicability:	Description:	Notes:
Level 2	Before inserting removable media into a sensitive system, ensure the device is fully formatted or is a write-once device.	It is also important to use fully formatted drives (not quick format) to remove all information prior to use.

2.5.5 Configure Anti-Malware Scanning of Removable Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	Use of USB devices is very common in election systems. Therefore, it is critical that all external devices be scanned for malware prior to use.	8.4

2.5.6 Use USB Port Protectors on Unused Ports

Profile Applicability:	Description:	Notes:
Level 1	Cover all unused USB ports on endpoint devices with locks or tamper-evident port protectors to ensure unauthorized USB devices are not inserted into the device.	This is especially important for devices that are taken into less physically secure environments. It is also important to put tamper-evident seals on ports that do have a device plugged in to detect an attempt to swap a legitimate device with an illegitimate one.

2.5.7 Disable Access to USB Devices Where Possible

Profile Applicability:	Description:	Notes:
Level 3	Disable the use of USB devices on a system to completely remove the risk of removable USB media-based attacks.	This may not be feasible for all components. It should be feasible for servers and other devices that do not use USB-connected devices.

2.5.8 Use USB Write Blocker to Transfer Data Into Sensitive Systems

Profile Applicability:	Description:	Notes:
Level 3	USB Write Blockers allow a high-integrity system to read the content of a USB device while mitigating the risk of transferring any malicious payload.	These devices should be used when transferring data into the voting system or the voter registration system using removable USB media.

3 Software Applications

Technology solutions consist of a software application or applications that perform a business function according to their goals and objectives. These applications use the resources made available to them by their host endpoint and network to achieve their business function. Often, these applications will provide a user interface for interacting with users, but this is not always the case. Like the tip of an iceberg, what people see of a software application is only a small fraction of the application itself. Most enterprise applications will have many supporting applications, frameworks, or libraries that enable them to perform their job quickly and reliably. These other applications or libraries may be written specifically for this software solution, may be common commercial components, may be open-source components, or may be a lesser known third-party component.

Most applications written today start with a process of identifying and collecting reusable applications, frameworks, and libraries that provide common functionality and then proceed to build upon those components to create the unique application required by the project's goals and objectives. This process typically yields higher quality software faster than building everything from scratch. This concept of software reuse is extremely popular but has some security drawbacks. Notably, it is hard or impossible to vet all the components being reused in any new application. It is even difficult to track which components are being used and which components they use, etc.

Web-based software applications are typically developed with client/server architectures. As introduced in the Networking and Architecture section, there are two common client/server architectures known as two-tier and three-tier, referring to the number of places where parts of the solution are implemented. Depending on the approach, there will be a minimum of two, but often three, different types of technology deployed. These are often referred to collectively as the "technology stack" used to build the application.

First, all web-based applications will have a data layer to store persistent data—almost always done with a relational database. There are many relational database options that range in cost and capability. Most have good security configuration options, but it is up to the developer to determine how to use them. The data layer will often also have file storage. File storage approaches can range from using typical file storage on the server, using network-attached storage, or using a cloud hosting storage option. The security controls available for each will vary based on the approach taken.

Second, all web-based applications will also have an application written in a high-level programming language such as Python, Java, C#, or scripting languages such as PHP. These applications are responsible for responding to HTTP requests and implementing the business logic. They rely on their programming language framework and many other libraries to build out their functionality. To assist with their responsibilities, there may also be separate applications that handle background tasks that are too intensive for the main application.

Finally, most web-based applications will utilize HTML, CSS, and JavaScript to implement a user interface that can be rendered in a web browser. It is important to understand how these technologies work together to constitute a web-based software solution and the security considerations for each.

Threats

There are many threats to the software applications. This list and discussion below are adapted from a report from the Cloud Security Alliance on the top threats to cloud computing (https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf).

Data Breaches

A data breach is an incident in which sensitive, protected, or confidential information is released, viewed, stolen, or used by an individual that is not authorized to do so. A data breach may be the primary objective of a targeted attack or may simply be the result of human error, application vulnerabilities, or poor security practices. A data breach may involve any kind of information that was not intended for public release including, but not limited to, personal and business information such as personal health information, financial information, trade secrets, and intellectual property.

Insufficient Identity, Credential, and Access Management

Data breaches and other attacks can occur because of a lack of scalable identity access management systems, failure to use MFA, weak password use, and a lack of permission checking.

Insecure Interfaces and APIs

Most web-based software applications expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with services. Provisioning, management, orchestration, and monitoring are all performed with these interfaces. Insufficient input validation or access control on these APIs can lead to many types of malicious activity depending on the capabilities of the API. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the internet are the first line of defense and detection.

Software Vulnerabilities

Software vulnerabilities are exploitable bugs in programs that attackers can use to perform unauthorized activity such as stealing data, taking control of the software, or disrupting service operations. Some vulnerabilities allow for the attack to deface the application and trick other users. Captured most prominently by the Open Web Application Security Project (OWASP), there are numerous types of software flaws that can result in allowing a malicious entity to execute an attack. These are known as the OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project). To handle the growing number of software vulnerabilities, there is a community-developed list of common software security weakness known as the CWE (https://cwe.mitre.org/).

Account Hijacking

Account hijacking is when an attacker can impersonate a legitimate user and take control of their account. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities allow this to happen. Credentials and passwords are often reused, which amplifies the impact of such attacks. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect other users to illegitimate sites. A compromised account or service may also become a new base for attackers. From there, they may leverage the power of the victim's reputation to launch subsequent attacks.

Governance

Software applications typically have a single entity responsible for developing and maintaining the application. They may have subcontractors and they will likely rely on other third-party components, but there is one entity to interact with to handle support and maintenance issues. This can be complicated if the original developer is no longer in business or available.

Depending on how the software application license was purchased, an election jurisdiction should have different expectations. First, software has historically been sold as "packaged" software. This is a situation where you buy the software at a moment in time. You have the option to purchase newer versions of that software for additional incremental cost. Some offerings have support and maintenance plans that offer these updates if you are within your maintenance period. Without the support and maintenance plan, the user is left to troubleshoot and create workarounds themselves. Customers should only expect security and feature updates if they purchased support and maintenance. Customers cannot control what is included in an update but can control when the upgrade is applied to their environment. This model is becoming less popular.

The second common arrangement is called Software-as-a-Service, or SaaS. This has multiple meanings and often implies as much about the technology as it does about the licensing model. Considering just the licensing model, a SaaS model allows an election jurisdiction to purchase the software license on an ongoing basis where the jurisdiction is always provided the latest version of the software. While the SaaS model often involves monthly fees, many election technology providers front-load these regular fees or convert them to annual fees to better accommodate how election jurisdictions purchase technology. This type of model has become extremely popular with web-based software. Most of the time, this model includes technical support. Some models offer licensing tiers where product functionality and technical support are available at graduating degrees depending on the licensing tier purchased. With any of these approaches, customers should expect regular security and feature updates but will often not have control over when these are applied to their environment.

Both the packaged and SaaS licensing models are used for commercial software applications. Custom software applications are very different, and the arrangements vary with every deal. Determining whether to purchase a commercial application or commissioning a custom software application depends on several factors including budget, control, and availability of features. Custom software applications will be significantly more expensive but will offer more control and capability to meet the jurisdiction's unique needs. Commercial software applications will be less expensive but offer less control over the product roadmap. With a custom application, the jurisdiction can control the product roadmap and can often control the level of resources dedicated to it. With a commercial application, the software developer must balance the needs of multiple customers when building their product roadmaps and assigning resources.

3.1 Secure Programming

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: failure to check the size of user input, failure to filter out unneeded but potentially malicious character sequences from input streams, failure to initialize and clear variables, and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.

There is a flood of public and private information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow "weaponization" of vulnerabilities into exploits. Attackers can inject specific exploits, including buffer overflows, Structured Query Language (SQL) injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. Many more web and non-web application vulnerabilities are discovered on a regular basis. It is more critical now than ever to ensure that applications source code is free—as much as possible—from the types of coding errors that create these vulnerabilities.

Many of the best practices provided in this section were adapted from the work by SANS Software Security group. SANS Software Security focuses the resources of SANS on the growing threats to the application layer by providing training, certification, research, and community initiatives to help development teams and security professionals build secure applications. They are an excellent resource for more information on software security (https://software-security.sans.org/).

Election Technology Application

Internet-connected election technology uses the internet to interact with voters over disparate geographic locations. Whenever it does this, it exposes sections of the application to the internet and exposes any underlying software vulnerability to attackers. Malicious actors look for these points of exposure and will evaluate whether those points have software vulnerabilities as one of the best and easiest ways to attack a system. Some of these tests are passive and hard to detect. Others are active and can be detected by monitoring systems. This activity is documented in the Mueller Report to have happened in the 2016 election and is a common technique of malicious actors. Moreover, these attacks are not expensive to wage and are often available using commonly accessible tools. On the other side, it is very difficult to ensure that a large election technology application is free from all programming flaws. Therefore, it is critical that only the minimum surface area of an application is exposed to the internet, and that the exposed area is free from software vulnerabilities as much as possible.

This section covers the specific actions to help secure source code. The next section covers the software development process required to ensure the source code remains as secure as possible.

3.1.1 Store and Communicate Data Securely

Profile Applicability:	Description:	Notes:
Level 1	Protect data by limiting its storage and transport, using the latest secure protocols and configuration, and requiring access over trusted encrypted channels.	See Appendix A: Secure Programming for data protection best practices.

3.1.2 Use the Latest Best Practices for Identifying and Authenticating Users

Profile Applicability:	Description:	Notes:
Level 1	Use strong authentication mechanisms, securely store credentials, don't hardcode passwords, and carefully design authentication mechanisms to not leak information about users.	See Appendix A: Secure Programming for authentication best practices.

3.1.3 Use Best Practices for Securely Handling Input and Output

Profile Applicability:	Description:	Notes:
Level 1	Validate and authenticate input, set proper encodings and secure headers, and use technology and coding practices that prevent injection attacks.	See Appendix A: Secure Development for input and output handling best practices.

3.1.4 Deploy Appropriate Access Control Mechanisms

Profile Applicability:	Description:	Notes:
Level 1	Ensure access control is consistently applied, follows the principle of least privilege, and prevents privilege escalation.	See Appendix A: Secure Programming for access control best practices.

3.1.5 Manage Secure Sessions With Users

Profile Applicability:	Description:	Notes:
Level 1	Ensure that user sessions are created and managed using secure cookies and unique session identifiers that are destroyed when users log out or are logged out after idle periods.	See Appendix A: Secure Programming for session management best practices.

3.1.6 Log Critical Information and Handle Errors Gracefully

Profile Applicability:	Description:	Notes:
Level 1	Ensure the application securely logs sensitive actions in appropriate detail and handles errors gracefully without revealing sensitive details to users.	See Appendix A: Secure Programming for error handling and logging best practices.

3.2 Application Development

CIS Control 18: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Election Technology Application

Election software providers are typically smaller organizations that specialize in election technology. While some larger companies exist, it is common for election technology companies to struggle with the concept of a Secure Development Lifecycle (SDL). It seems daunting and something only larger companies can manage. While it is true that larger companies have an advantage, many aspects of this section are achievable by small companies that are willing to devote the resources to decreasing the risk of vulnerabilities in their products.

No matter the size of the organization, two key concepts of an SDL should be prioritized and implemented. The first is security testing that includes vulnerability scanning. The organization should acquire software that runs vulnerability scans against the software to look for common coding flaws that materialize as software vulnerabilities. There are many options available at various price points with varying degrees of competency. This type of vulnerability testing focuses on software programming flaws as opposed to vulnerability scanning, the latter of which focuses on detecting outdated or unpatched software running on the web servers. The second critical SDL aspect is change management. All code changes, check-ins, and publishes should be tracked with details on what was changed and who changed it. This prevents someone from inserting malicious code without accountability. Once this is established, it is much easier to enforce code reviews and roll back to prior versions if necessary.

3.2.1 Establish Secure Coding Practices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Establish secure coding practices appropriate to the programming language and development environment being used.	OWASP provides some useful programming language-specific cheat sheets that may be helpful in creating secure programming practices. https://github.com/OWASP/CheatSheetSeries.	18.1

3.2.2 Establish a Rigorous Change Management Process

Profile Applicability:	Description:	Notes:
Level 1	A rigorous change management process must be maintained during change management operations. New releases should only be deployed after the process is complete.	This prevents a single person from making a change to the software and deploying it without leaving a record of their change.

3.2.3 Define Security Requirements and Bake In Security

Profile Applicability:	Description:	Notes:
Level 1	The election technology provider should define security requirements for the application. This includes items that range from the whitelist validation rules all the way to nonfunctional requirements like the performance of the login function. Defining these requirements upfront ensures that security is baked into the system.	Every development iteration should attempt to address one or more security-related feature or control. Security demands continual evaluation, so election technology providers should plan to make security-related changes every release.

3.2.4 Ensure Software Development Personnel Are Trained in Secure Coding

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that all software development personnel—software developers, testers, and architects—receive training in writing secure code for their specific development environment and responsibilities.	Most application level threats can be mitigated by writing defensive code. Election technology should be coded in a defensive manner.	18.6

3.2.5 Conduct a Design Review

Profile Applicability:	Description:	Notes:
Level 1	Integrating security into the design phase saves money and time. Conduct a risk review with security professionals, and threat model the application to identify key risks. This helps you integrate appropriate countermeasures into the design and architecture of the application.	DREAD and STRIDE are application threat modeling techniques that offer structured approaches to identify, classify, rate, compare, and prioritize the security risks associated with an application. Federal partners, state officials, and third-party consultants are available to review election system designs and provide feedback early into the process to ensure the proper approach to security. Design reviews should be done for new and existing products.

3.2.6 Perform Code Reviews

Profile Applicability:	Description:	Notes:
Level 1	Security-focused code reviews can be one of the most effective ways to find security bugs. Regularly review code for common issues like SQL Injection and Cross-Site Scripting vulnerabilities.	Employ automated code analysis tools where possible. When reviewing results and doing manual reviews, rotate reviewers periodically to avoid collusion and fatigue.

3.2.7 Perform Security Testing

Profile Applicability:	Description:	Notes:
Level 1	Conduct security testing both during and after development to ensure the application meets security standards. Testing should also be conducted after major releases to ensure vulnerabilities did not get introduced during the update process.	Internal quality assurance activities should be followed for all releases. External testing, even when not required, should also be done on releases, especially major releases.

3.2.8 Apply Static and Dynamic Code Analysis Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	These tools can run on every code check in and should be a part of the change management workflow. Violations should be investigated and corrected when necessary.	18.7

3.2.9 Verify That Acquired Software Is Still Supported and Hardened

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	Efforts should be made to use only supported and hardened software for election technology systems.	18.3

3.2.10 Establish a Process to Accept and Address Reports of Software Vulnerabilities

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Vulnerabilities may be uncovered internally or externally. Election technology providers should have a system to categorize and respond to vulnerability reports.	18.8

3.2.11 Only Use Up-to-Date and Trusted Third-Party Components

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Only use up-to-date and trusted third-party components for the software developed by the organization. Follow supply chain security best practices.	Establish trustworthiness of suppliers by following appropriate supply chain security guidance. Consider working with third-party software suppliers to understand their roadmap and get ahead of any change in their support and security patching process.	18.4

3.2.12 Automate Application Deployment

Profile Applicability:	Description:	Notes:
Level 3	Automating the deployment of your application with continuous integration and continuous deployment can help to ensure that changes are made in a consistent, repeatable manner in all environments.	This can reduce overhead and ensure that all changes are tracked in the source code repository for auditing and troubleshooting purposes.

3.2.13 Separate Production and Non-Production Systems

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	There should be a formal signoff by election officials, or their representatives, to move changes from the test environment into production. The same people who make the changes should not be allowed to move changes into production.	18.9

3.2.14 Deploy Web Application Firewalls (WAFs)

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Protect web applications by deploying WAFs that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	These can be very effective at protecting multiple web applications at once. This should be considered for web deployments of multiple election applications in the same hosting environment.	18.10

3.2.15 Use Only Standardized and Extensively Reviewed Encryption Algorithms

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Use only standardized and extensively reviewed encryption algorithms.	Use standard libraries available from reputable sources instead of developing your own cryptographic solutions.	18.5

3.2.16 Use Standard Hardening Configuration Templates for Databases

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	For applications that rely on a database, use standard hardening configuration templates. Systems should be tested to ensure hardening did not break functionality.	The CIS Benchmarks are available for various database offerings such as SQL Server, MySQL, and PostgreSQL. Guidance for cloud-based databases is also available.	18.11

4 Data

An organization's level of risk is related to the sensitivity of the data it processes or possesses. Your data is often the most valuable thing you handle and is most often the target of the adversary's efforts. This is evident in the number of data breaches being reported today from large corporations with personal information and protected health information (PHI). This is also why there are laws or rules in place for organizations that handle this data.

Election data is just as—if not more—sensitive. Some election data is personal information, some is critical for election integrity, and some is both. Nearly all election data has value to an adversary, but the value of a successful attack can be very time-dependent, impacting a specific function and point in time.

The following sections review some of the most critical election data elements, identify the typical lifecycle for that data, and discuss the points where its value is the highest.

Jurisdictional

Jurisdictional data is persistent and defines an election jurisdiction. This includes information about the structure of the jurisdiction such as districts, precincts, and offices. This information is often contained within the county voter registration or election management system and shared with other systems that consume it. When elections are built, a snapshot of this information is used to help define the election. This data is key to building correct ballots and ensuring that voters can vote for the correct candidates and issues. The jurisdictional data used to assign ballot contents to the correct geographical districts and polling places is most at risk when it is used to build the ballots and assign them. This puts the entire supply chain of that data leading up to ballot generation at risk.

Voter

Voter information is persistent data that identifies eligible voters and their attributes to help the county interact with each voter. This data is managed in the state or county voter registration systems. Depending on the state, the data flow between state and county voter registration systems varies with the consistent goal of keeping both systems in sync. Voter data is then consumed by various software applications that interact with voters. This includes electronic pollbooks, electronic ballot delivery systems, online voter registration portals, sample ballot lookup portals, and others. Only certain fields—not the entire voter record—are shared with these other software applications.

Voter information has full, filtered, and public versions. In most states, registering to vote requires the sharing of personal information such as Social Security number (SSN) and driver's license number. These data elements combine with the voter name, address(es), and other attributes to constitute the full version of the voter record. Most states consider voter registration records to be public, but some of the sensitive information such as SSNs are redacted. This version is known as the public version. Various other filtered formats are available for products that use voter information. For example, electronic pollbooks may require voter records with the driver's license number but not the SSN. Distinguishing between these versions is important when discussing risks.

Full voter records are at risk throughout their lifecycle due to their value in perpetuating identity theft. They are also in danger of manipulation in the voter registration system because it is the source of voter records for all other systems. Other forms of voter records used for voter eligibility are at most risk of manipulation or deletion when they are transferred and used in electronic ballot delivery or electronic pollbooks. Even though certain sensitive data fields are removed, the data is still extremely valuable for an attacker who may wish to alter a voter's eligibility to vote or impact for whom they can vote. While these downstream uses of voter records could always refresh themselves from the voter registration database, a well-timed attack on the local version of the voter records could be very impactful.

Election

Election data is a combination of jurisdictional information, candidate filing information, and other attributes. Elections are defined by the offices and issues that will appear on the ballot along with their eligible candidates and options. Though there is no definitive composition, many refer to the election data as the election definition. Each technology implementation will have a unique specification for an election definition.

Typically, the Election Management System (EMS) creates the election by combining disparate pieces from multiple systems. The term EMS is itself used differently in various places. In some instances, the EMS is an online system often embedded in the voting registration system where the state and counties collaborate to define the election or parts of the election.

In other instances, there is a component of the county voting system that is called the EMS. This is the part of the voting system that finalizes the election and builds the ballots. In all cases, the term refers to a system that contributes to the definition of the election in part or in whole. Also, consistently, the EMS is responsible for communicating the election definition with various consumers. These consumers include public communication channels, ballot marking devices, ballot tabulators, and ballot printers.

Election definitions created by voting systems typically define the construction of the ballots and the rules by which poll workers and voters interact with the ballots. In some cases, the election definition may also include configuration data for election security— keys, passwords, PINs, etc.—and how to tabulate ballots. The election definition is what is used to program the various technology components of a voting system. Once the election definition is created and approved by the jurisdiction, its integrity has critical value. Modifications to the election definition can significantly alter how the election is conducted and the outcome of the process.

Ballot (Blank)

Ballot data is the collection of ballot contents into ballot styles and may take the form of structured data or printable forms like PDFs. Ballot data is a subset of election data but is separated for our purposes because you will often find ballot data isolated from election data. When isolated from election definitions, ballot data has a unique risk profile. Ballot data is often created by the voting system's election management function and is then distributed to various consumers. This includes ballot printing companies, on-demand ballot printers, ballot marking devices, and electronic ballot delivery systems.

Modification of blank ballots can disenfranchise voters or manipulate how their intent will be read by the voting machine tabulators. For example, a blank ballot could be altered to switch the order of candidates. The election definition is programmed to read the ovals in the original order, but the voter marks the ovals according to what they see on their ballot. This will cause their vote to be attributed to the wrong candidate. Blank ballots are most at risk from the time they are approved by the election jurisdiction to when they are presented to the voter for marking.

Election Results

Election results are the aggregated totals generated from voting system tabulation functions. These typically come in summary and detailed versions. The most common detailed version is precinct-level results, but this may also refer to results by district. Election results are generated by the voting system in various individual machines and then aggregated into a central result reporting function of the voting system. Election results are initially considered "unofficial" and then go through a canvassing process that will certify the results as official. The canvassing process differs based on state law and by office.

Most people recognize the lifecycle of election results as beginning when the polls close on election night. In fact, the lifecycle begins when the first ballot is cast in the election, which may be weeks before Election Day. As soon as the first ballot is scanned, the tabulator will store results—including a ballot image in most systems. The results are maintained and updated on individual machines until they are aggregated by the election jurisdiction. Typically, the election jurisdiction will wait until polls close on election night to aggregate results from the individual tabulators into a results reporting system. This can be done one of three ways. First, the results can be manually entered from results tapes. Second, the removable media from the tabulator can transfer the results to the results reporting system. Third, the results may be remotely transferred from the tabulator. The last option is only available in some states and is only used for tabulators used on Election Day.

Once an election jurisdiction aggregates the results it has when polls close on election night, those results are transferred from the voting system to an election night reporting solution. The voting system is typically offline, and the election night reporting solution is an online system. This transfer is typically done using USB-based removable media. Once the results are on an election night reporting solution, they are made available to the public using an election night reporting website. For the most part, the risk to election results is the risk to their integrity. However, it is equally important to protect the confidentiality of election results prior to polls closing.

Election night results are a form of unofficial election results. Those results are special because they don't go through rigorous review, are stored and displayed from internet-connected web servers, and are sometimes aggregated from results sent by vote tabulators over public networks. Nevertheless, they are immediately trusted by the public. As such, these results are at significant risk of tampering and manipulation. The outcome of such tampering would lead to widespread confusion and distrust in the correct result produced by the voting system.

Threats

The following are threats that should be considered when evaluating how to best secure sensitive data.

Data Leakage

Data leakage occurs when information is exposed as the result of an organization's internal processes or by a mistake. This is done by internal actors who mistakenly send or store information without the proper protection.

Data Breach

Data breaches are intrusions into sensitive systems and an extraction of their data. A data breach is often the result of a cyberattack that allows the attacker unauthorized access to a computer system or network, enabling them to steal the private, sensitive, or confidential data contained within. In a data breach, the attacker not only gains access to the data but is able to exfiltrate the data outside of the original system. Data breaches can be achieved using many tactics, such as spyware, exploiting a software vulnerability, phishing, misconfigured access controls, etc.

Data Manipulation

Data manipulation occurs when authentic data is altered by an unauthorized actor. The motivation for data manipulation may be financial, reputational, or criminal. Web defacement is an example of a data manipulation attack. For this attack, the actor can access the data with the permissions to alter it in its official location. This can be accomplished by exploiting software vulnerabilities, gaining access to the organization's network assets, privilege escalation, and other methods. If possible, sophisticated attackers will alter data backups in addition to or instead of primary data.

Data Loss

One type of data manipulation attack is data loss. Instead of modifying the data, the data is deleted from the server. Ransomware is a form of data loss where the data is manipulated to become unusable without the encryption key. Again, the attacker may also delete data from backups in sophisticated versions of this attack.

Governance

Data governance is the overall management of the availability, usability, and integrity of data. A sound data governance program includes a defined set of policies and procedures for how to handle certain data. A full data governance program will also include data classification and data lifecycle management.

Data classification is extremely important. If all data is treated the same, the organization will become too resource constrained and truly critical data will go without the proper protection. Therefore, it is very important to classify data based on its value, or sensitivity. From this classification, administrative and technological controls can be deployed based on the data's sensitivity. One challenge in data classification is training personnel to recognize and label data based on sensitivity. To combat this challenge, choose a classification scheme that is simple yet effective.

Data lifecycle management builds upon data classification. The activities and controls for each phase of the data's existence will be defined by the sensitivity of that data. There is no set of definitive data lifecycle phases but generally there are six: generation/capture, maintenance, active use, publication, archiving, and purging.

Election jurisdictions should look to organize a data governance strategy that includes both data classification and data lifecycle management. This program should be communicated with staff, vendors, and partners to ensure they are compliant with the policies and procedures that govern your data.

4.1 Data Protection

CIS Control 13: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Election Technology Application

Most data classification and security controls focus on data confidentiality. For election technology, data classification should include consideration for the impact on the election if the confidentiality or integrity of the data were compromised. One approach is to create a classification scheme that simultaneously identifies the confidentiality and integrity of the data—examples include "confidential, high integrity" and "public, high integrity."

Identifying the confidentiality and integrity is important and will assist in determining the proper controls for that data. For example, election night results are public, but to solely classify that data as "public" might imply it is low-integrity data. Instead, classifying it as "public, high integrity" makes clear the importance of keeping the data protected but visible.

Additionally, election data goes through changes in classification throughout the election and this must be accounted for in the data classification scheme. For instance, election results prior to the polls closing are "confidential, high integrity" and are changed to "public, high integrity" when polls close.

4.1.1 Maintain an Inventory of Sensitive Information

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including information located onsite or at a remote service provider.	Locate all data that has privacy concerns and election operations concerns if its confidentiality or integrity were to be compromised.	13.1

4.1.2 Remove Sensitive Data or Systems Not Regularly Accessed by the Organization

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems should only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Disconnect systems that store or process election data that do not absolutely have to be online. Do not leave USB devices with sensitive information plugged into machines when they are not in use.	13.2

4.1.3 Monitor and Block Unauthorized Network Traffic

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security personnel.	Deploy and configure Data Loss Prevention (DLP) solutions to look for election and voter related information that should not be leaving your network boundaries.	13.3

4.1.4 Monitor and Detect Any Unauthorized Use of Encryption

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	Data breaches will often try to exfiltrate data through encrypted channels. Monitor and prevent the use of unauthorized encrypted channels.	13.5

4.1.5 Encrypt the Hard Drives of All Mobile Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Use approved whole disk encryption software to encrypt the hard drives of all mobile devices.	Determine what sensitive information you will permit on employees’ laptops and mobile devices. Ensure the hard drives of laptops and mobile devices are fully encrypted to prevent information from being stolen.	13.6

4.1.6 Manage USB Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	If USB storage devices are required, enterprise software should be used that can configure systems to allow only the use of specific devices. An inventory of such devices should be maintained.	Only authorized USB devices should be used on trusted, high-integrity election systems. When using a device on a trusted system, ensure it has been fully wiped before use. For information transfer between an untrusted system and a high-integrity system, ensure the USB device is scanned for malware before inserting into a high-integrity election system.	13.7

4.1.7 Manage System's External Removable Media's Read/Write Configurations

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Configure systems to not write data to external removable media, if there is no business need for supporting such devices.	This prevents someone with physical access to a system storing sensitive information from extracting that information onto a USB drive.	13.8

4.1.8 Encrypt Data on USB Storage Devices

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	Data classified as confidential should be encrypted whenever it is stored on a USB device.	13.9

4.2 Controlled Access Based on Least Privilege

CIS Control 14: 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 and modify these critical assets based on an approved classification.

Election Technology Application

Most data within elections is available to many parties but is only editable by a few. Therefore, organizations must establish access controls with the proper view and modify permissions. Ensure that data storage and data processing solutions offer you the ability to give users permissions for viewing data separate from editing the data. Then, ensure that each user's account is properly set up accordingly. This can be done efficiently using systems that implement role-based access control.

4.2.1 Protect Information Through Access Control Lists

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Protect all information stored on systems with file system, network share, claims, application, or database-specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Identify the roles of individuals in managing election data before identifying the minimum privileges necessary for them to do their job. Avoid giving administrative access to more people than necessary, while also not creating single points of failure.	14.6

4.2.2 Digitally Sign Sensitive Information in Transit

Profile Applicability:	Description:	Notes:
Level 1	Sensitive data should be digitally signed by its originator and verified by all components which read, store, or process the data.	The integrity of election data must be maintained throughout its lifecycle. While data should be digitally signed data in transit, a stronger approach is to establish a chain of integrity proofs throughout its lifecycle.

4.2.3 Encrypt All Sensitive Information in Transit

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Encrypt all sensitive information in transit.	Consider whether the election data's confidentiality is sensitive. If you are unsure, consider it sensitive.	14.4

4.2.4 Encrypt Sensitive Information at Rest

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Election databases and their backups, for example, should be encrypted to ensure they are protected from manipulation.	14.8

4.2.5 Segment the Network Based on Sensitivity

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Segment the network based on the label or classification level of the information stored on the servers, and locate all sensitive information on separated Virtual Local Area Networks (VLANs).	Consider establishing unique networks for each election technology and service offering.	14.1

4.2.6 Enable Firewall Filtering Between VLANs

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	Segmenting the network and preventing movement across boundaries can stop an attack on less sensitive data from accessing more sensitive election data.	14.2

4.2.7 Disable Workstation-to-Workstation Communication

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Using technologies such as private VLANs or micro-segmentation, disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems.	Whenever possible, workstations should be limited to talking only to servers.	14.3

4.2.8 Utilize an Active Discovery Tool to Identify Sensitive Data

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	This helps an organization find and secure all instances of sensitive election information.	14.5

4.2.9 Enforce Access Control to Data Through Automated Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system.	This will help ensure sensitive data that is not properly labeled is still protected from leaving its host system.	14.7

4.2.10 Enforce Detail Logging for Access or Changes to Sensitive Data

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Enforce detailed audit logging for access to sensitive data or changes to sensitive data using tools such as File Integrity Monitoring or Security Information and Event Monitoring.	This can help detect a malicious attempt to alter the integrity of the data. Database level logging can be enabled to track all changes to the database.	14.9

4.3 Cloud Storage Configuration

Cloud storage options are offered by the major cloud service providers. These services offer a way to store non-relational data of various sizes and formats in a highly available environment. These services replace local or network file storage solutions and are accessible through an API instead of traditional file system exploration.

It is very common for web applications hosted by a cloud service provider to use cloud storage. It is also very common for organizations to use cloud storage for large amounts of data that needs to be accessible from the web. Cloud storage provides protections against ransomware and other intentional or unintentional manipulation. Cloud storage, however, has often been the source of data breaches that take advantage of missing or insecure security permission configurations. It is not that cloud storage doesn't offer highly secure options, but it is often difficult to ensure you have fully and properly set all of the correct configuration settings.

Election Technology Application

Storing election data in a cloud storage environment requires consideration of security measures, especially if the data is for a current election. There are many advantages to cloud storage for performance and availability reasons, and there are many use cases where it makes sense to use it. For example, archived election data for researchers and press is a good use for cloud storage as the data may be very large in size and publicly available after the election.

When considering the use of cloud storage, first consider whether the same result can be achieved with a local storage option. For example, if the information is only needed internally, using a cloud storage container may not be necessary. Whenever possible, try not to expose sensitive election data to a cloud storage environment. For applications where storage of large amounts of data, fast response times, or high availability are necessary, cloud storage may be a good solution and the best practices in this section should be used to ensure your cloud storage container(s) are properly configured to prevent or mitigate a data breach.

4.3.1 Follow Secure Configuration Guidance for Cloud Storage

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Follow guidance from CIS Foundations Benchmarks or other secure configuration guidance to ensure all cloud storage containers with sensitive election data are properly secured.	CIS Foundations Benchmarks are available for Amazon Web Services®, Microsoft Azure®, Google Cloud®, and Microsoft® Office 365.	5.1

4.3.2 Encrypt Data Stored in Cloud Storage Containers

Profile Applicability:	Description:	Notes:
Level 2	Use application encryption with secret keys only known to the data owner(s) to protect confidential data stored in a cloud storage container.	This protects the data even in the event of a data breach of the cloud hosting provider or a misconfiguration of the cloud storage container's permissions.

4.3.3 Routinely Audit Cloud Storage Configuration Settings

Profile Applicability:	Description:	Notes:
Level 1	On a periodic basis, review configuration settings for all cloud storage containers and match their effectiveness to the sensitivity of the data being stored in the container.	Automated routines are available for evaluation against the CIS Foundations Benchmarks. Automated routines may be necessary if you have a lot of containers.

4.3.4 Use Separate Storage Containers for Unique Data Classifications

Profile Applicability:	Description:	Notes:
Level 2	Don't overload one container with data at multiple classification levels. Create separate containers with appropriate names and configuration settings for each data classification level.	Follow your data classification scheme and establish containers based on sensitivity. Also, don't mix production and test data or data from different technologies and products.

4.3.5 Avoid Using Email to Store Sensitive Data

Profile Applicability:	Description:	Notes:
Level 1	As much as possible, avoid emailing sensitive data and avoid using email inboxes for storage of sensitive information.	Use alternative, more secure methods of sending and storing sensitive election information such as secure FTP sites and encrypted web portals.

5 Administration

All technology is provided by, maintained, and ultimately protected by a combination of technology and people. Oftentimes, the people who develop the technology are not the same people who deploy and administer it. This is why administration security controls are separated from the other areas. These organization-level best practices focus on the activities that extend beyond the technological boundaries and into areas predominantly controlled by people and processes. This section is not an exhaustive list of the best practices in this area, but it covers some of the more important controls.

Election organizations need to be concerned with how people and processes within their organization affect the security of the election. This must first begin with ensuring that you can detect a security incident. This is done with robust audit logging and monitoring. It is also assisted by employees who are aware of their responsibilities to be active participants in election security. This means they must know the types of threats they may be asked to recognize and resist. Each person with a role in developing, testing, deploying, or managing election technology must recognize they may be a target or may be in a position to recognize an attack, if not prevent it. Their understanding and vigilance, along with supportive technology and logging, are critical to prevention and early detection.

Perhaps just as important as detecting and preventing attacks is incident response. Each technology provider, service provider, and election jurisdiction should have incident response plans that are vetted and tested on a regular basis. This should extend beyond the typical service outage incident into more complicated and persistent types of incidents, such as an advanced persistent threat. One of the key things to plan for is communication: knowing what you will do internally, who you will reach out to for help, and how you will communicate with the public. Organizations should also make sure that they have made arrangements to have the services and data you will need to recover from an incident. This may involve setting up relationships and contracts ahead of time and establishing data and system backups.

Threats

This section addresses the threats that are best mitigated with organizational-level controls.

Social Engineering

Social engineering attacks are one of the more common and successful types of attacks. This is because they prey upon human tendencies and emotions. A successful social engineering attack can have devastating impacts on an organization. While these types of attacks are often preventable, they are getting more and more sophisticated and harder to identify. This is why it is important for employees to know what to look for and how to spot suspicious activity in their email, over the phone, and even in person.

Social engineering attacks include phishing, spear phishing, vishing, pretexting, baiting, tailgating, and quid pro quo. Phishing is the most common type of social engineering attack. The attacker recreates the website or support portal of a renowned company and sends the link to targets via emails or social media platforms. The other person, unaware of the attack, ends up revealing personal information, credit card details, or other sensitive information. Another form of phishing will trick the user into navigating to a website that downloads malicious software.

Social engineering attackers are best defeated by an aware and skeptical employee base. Employees need to be aware of their tendencies and maintain a healthy skepticism of any communication that is not from a trusted, known party. Employees also need to ensure that the sender of a communication is authentic. Holding regular social engineering awareness trainings and distributing regular corporate communications that show examples of social engineering attacks are good tactics. Employees learn best from seeing examples of the phishing emails. Role-playing is another good tactic to use to combat vishing and pretexting attacks. Often, in vishing type attacks, the attacker will attempt to connect with the employee and make an emotional plea for the employee to circumvent standard security to help them quickly. Role-play training for employees exposes them to this type of tactic and helps reinforce appropriate responses in real-world scenarios.

Insider Attack

All technology is developed, tested, deployed, and maintained by humans. Many technological controls can mitigate the risk of an insider attack, but it can never be fully prevented by technology alone. Trusted employees can become malicious over time or nefarious actors may attempt to infiltrate an organization. A combination of procedural and technological controls should be used to detect possible insider threats.

Insider threats do not have to be from employees. They may also come from former employees, contractors, or business associates who have inside information concerning business practices, data, or computer systems. Having a robust vetting process during the hiring and termination processes will mitigate much of the risk associated with insider threats. However, the organization should also consider an employee monitoring program to identify suspicious behavior of current employees.

Governance

The importance of security must be led by management and reinforced throughout the governance structure of an organization. It begins with expressing the importance of security at the top of the organization and ensuring that it is properly resourced with people and money. The level of investment will vary based on the size of the organization, the type of election technology, and overall cybersecurity risk.

Each organization should identify a cybersecurity and risk management framework to use to govern their cybersecurity approach. Furthermore, it is important to have a single individual within the organization serve as the primary cybersecurity point of contact. In larger organizations, this is often a Chief Information Security Officer. In smaller organizations with less critical operations, it may not necessitate a full-time role. No matter the size of the organization, this individual should have as much expertise in security as possible. Furthermore, this person should be given the authority to make an internal assessment of the organization's security without fear of reprisal from peers or management. An open and honest internal conversation about security weaknesses is critical to ensuring the organization is properly managing security.

When looking at an organization's security governance structure, it is important to structure roles and responsibilities such that more than one person is required to perform critical operations. This is called segregation of duties and reduces the likelihood that one person could both execute and cover up a cybersecurity attack. For example, the same people developing software should not be the same people deploying and auditing the software. This principle goes together with the principle of least privilege. Least privilege should be used when establishing user permissions. Users should only be given the permissions necessary to perform their responsibilities, and no more.

5.1 Account Monitoring and Control

CIS Control 16: Actively manage the lifecycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Election Technology Application

Election technology accounts must be properly managed and maintained. Establish periodic audits of accounts to ensure that only persons with a current need to use the system have active accounts. This is also a good time to review the permissions assigned to users. Permissions "creep" is very common in software applications, and without routine maintenance, user permissions will only increase and rarely decrease. It is important to remind users that taking away permissions is not performance-related or personal, it is a prudent security measure.

As discussed in the Data section, the permissions should be established based on the data classification and what you are trying to protect. For example, it is important to only have certain users who can upload and modify election night results or modify ballot styles in an electronic ballot delivery system. In these high-integrity systems, it is important to limit the number of users who have these permissions.

While it is ideal to always have unique accounts tied to unique individuals, it is not always possible. Sometimes shared accounts are required, such as a poll worker account. It is reasonable to only have a few poll worker accounts that share the same password for poll worker usability and training. This approach, however, introduces significant risk that the shared password will get into the wrong hands. To address this, shared accounts should be given the absolute lowest level of permissions possible and the poll worker account password should be changed frequently, with a minimum of every election. Never share administrator accounts.

5.1.1 Maintain an Inventory of Authentication Systems

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	Make sure you have a full understanding of how all users are authenticated and by what mechanism. It is possible for the same application to have multiple login pages. Make sure you know about these.	16.1

5.1.2 Configure Centralized Point of Authentication

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	This makes it easier to ensure all users are being properly authenticated with the appropriate level of scrutiny and can centralize authentication logging as well.	16.2

5.1.3 Require Multifactor Authentication

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Require MFA for all user accounts, on all systems, whether managed on-site or by a third-party provider.	This is one of the best protections against social engineering attacks.	16.3

5.1.4 Encrypt or Hash All Authentication Credentials

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Encrypt or hash with a salt all authentication credentials.	Ensure that local accounts and accounts with third parties use this approach to store your credentials, and try not to use the same password for third-party accounts and an election technology account. This will limit the impact of a third-party provider breach from impacting the election technology.	16.4

5.1.5 Encrypt Transmittal of Username and Authentication Credentials

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	This includes network traffic and data moved using removable media.	16.5

5.1.6 Maintain an Inventory of Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Maintain an inventory of all accounts organized by authentication system.	Maintain an up-to-date list of accounts for each system and tie each account to an individual person wherever possible.	16.6

5.1.7 Establish Process for Revoking Access

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling those accounts, instead of deleting accounts, allows preservation of audit trails.	Employee new hire, termination, promotion, and demotion checklists should include the steps to setting user permissions commensurate with the employee's job responsibilities, or lack thereof. This should apply to employees and contractors.	16.7

5.1.8 Disable Any Unassociated Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Disable any account that cannot be associated with a business process or business owner.	Try to document relevant business processes and owners to make auditing and maintaining accounts easier.	16.8

5.1.9 Disable Dormant Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Automatically disable dormant accounts after a set period of inactivity.	This is especially helpful for critical components of the election technology and will assist with the manual account audits that should be done on a periodic basis.	16.9

5.1.10 Ensure Temporary Accounts Have an Expiration Date

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that all temporary accounts have an expiration date that is monitored and enforced.	This best practice should be applied to contractor accounts and accounts that are meant to be temporary, such as election-specific accounts. It is OK for service accounts and employee accounts to not have an expiration date. Treat users as temporary whenever there is uncertainty.	16.10

5.1.11 Lock Workstation Sessions After Inactivity

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Automatically lock workstation sessions after a standard period of inactivity.	This is a basic security control that should be used universally. Employees should also be trained to lock their computers whenever they leave their devices.	16.11

5.1.12 Monitor Attempts to Access Deactivated Accounts

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Monitor attempts to access deactivated accounts through audit logging.	This can alert election system administrators to likely malicious behavior.	16.12

5.1.13 Alert on Account Login Behavior Deviation

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	Major commercial systems have the capability to establish an activity baseline based on time of day, IP address, and other data. Where possible, set up alerts to anomalous behavior for early detection of a possible attack.	16.13

5.2 Implement a Security Awareness and Training Program

CIS Control 17: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Election Technology Application

An effective enterprise-wide training program for election technology should take a holistic approach and consider policy and technology at the same time as the training of people. Policies should be designed with technical measurement and enforcement, and they should be reinforced by training to fill gaps in understanding. Technical controls can be implemented to protect systems and data and minimize the opportunity for people to make mistakes. With technical controls in place, training can be focused concepts and skills that cannot be managed technically.

An effective cyber defense training program is more than an annual event; it is an ongoing process improvement with the following key elements:

- The training is specific, tailored, and focused based on the specific behaviors and skills needed by the workforce, depending on their job role and responsibility. This should include training which is different for software developers, system engineers, technical support, etc.
- The training is repeated periodically, measured and tested for effectiveness, and updated regularly.
- It will increase awareness and discourage risky workarounds by including rationale for good security behaviors and skills.
- It will alert employees to the types of things to look out for, such as how to tell if a seal has been tampered with, and how to report suspicious events.

Here are some helpful links to training resources:

- The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to U.S. government employees, federal contractors, and veterans. https://fedvte.usalearning.gov/.
- Security engineering training by SAFECode is an online community resource offering free software security training courses delivered via on-demand webcasts. https://safecode.org/training/.

5.2.1 Perform a Skills Gap Analysis

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	Election technology has unique security awareness concepts that should be included in this gap analysis. This includes concerns around physical security and integrity protections, which are not always the focus of more generic security awareness programs.	17.1

5.2.2 Deliver Training to Fill the Skills Gap

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	Identify training providers, subject matter, and dates for training based on areas of highest need.	17.2

5.2.3 Implement a Security Awareness Program

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	This is the baseline information of common security attacks against employees using social engineering, how to identify such attacks, and how to adopt behaviors that will mitigate their effectiveness. This should be given to all permanent and temporary employees. Election-specific hiring should include this training.	17.3

5.2.4 Update Awareness Content Frequently

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.	Incorporate information from DHS and EI-ISAC alerts into training programs to ensure employees are aware of the latest tactics used by malicious actors.	17.4

5.2.5 Train Workforce on Secure Authentication

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Train workforce members on the importance of enabling and utilizing secure authentication.	Ensure employees are aware of the importance of creating unique, difficult to guess, but easy to remember passwords that they do not share with anyone.	17.5

5.2.6 Train Workforce on Identifying Social Engineering Attacks

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	This is a known tactic used to attack election technology providers and jurisdictions. Ensure all employees are aware of, and know how to spot, potentially malicious emails or phone calls.	17.6

5.2.7 Train Workforce on Sensitive Data Handling

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Train workforce on how to identify and properly store, transfer, archive, and destroy sensitive information.	Ensure all employees know how to identify and classify data at your various levels of classification. Once data is properly identified and classified, employees should be trained on how to properly handle the data at its classification level.	17.7

5.2.8 Train Workforce on Causes of Unintentional Data Exposure

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	The best form of protection is to train employees on what to NOT email, such as never emailing passwords.	17.8

5.2.9 Train Workforce Members on Identifying and Reporting Incidents

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	Incidents normally have warning signs that can lead to early detection. Training employees, particularly temporary elections staff, on what to look for and how to report can be very helpful in the event of malicious activity.	17.9

5.3 Maintenance, Monitoring, and Analysis of Audit Logs

CIS Control 6: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Election Technology Application

Capturing and analyzing activity on election technology helps detect and deter malicious activity. This includes capturing audit logs on network devices, network services, security devices, operating systems, and applications across all devices and networks. Most free and commercial technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers where possible. Firewalls, proxies, and remote access systems (e.g., VPN, dial-up) should be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems and applications, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges.

Election officials and election technology providers should periodically review audit logs or use a security information and event management (SIEM) solution. There are certain times that are more important than others to review logs. First, ensure that logs are reviewed prior to the beginning of sensitive election operations. This helps detect an intrusion attempt that may have placed unauthorized software or services on the network. Next, regular auditing throughout the election period is important to quickly detect and respond to an ongoing attack. Finally, a review of the audit logs after the election period helps ensure no suspicious activity was occurring. Any suspicious activity should be investigated and reported as quickly as possible. This may require assistance from others such as the Department of Homeland Security incident response team.

Analytical programs such as SIEM solutions can provide value, but even though the SIEM's audit log analysis is extensive, a basic examination by a person should also be done. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators.

5.3.1 Activate Audit Logging

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that local logging has been enabled on all systems and networking devices.	Components of election technology solutions must utilize local logging capabilities to store system activity.	6.2

5.3.2 Ensure Adequate Storage for Logs

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure that all systems that store logs have adequate storage space for the logs generated.	Election technology components should be designed to store audit logs for multiple significant election events without losing any data. Logs should be retained for a minimum of 180 days with the option to archive logs for longer periods of time.	6.4

5.3.3 Regularly Review Logs

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	On a regular basis, review logs to identify anomalies or abnormal events.	Election technology providers should ensure logs are reviewed prior to, during, and immediately after active election periods.	6.7

5.3.4 Deploy SIEM or Log Analytic Tools

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.	Timely and accurate detection of potential security events is critical during peak election periods. A SIEM solution can greatly assist with this.	6.6

5.3.5 Central Log Management

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Networked election technology solutions should utilize central event logging. Central event logging is extremely beneficial for detecting events and ensuring event logs are properly protected.	6.5

5.3.6 Enable Detailed Logging

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Enable system logging to include detailed information such as an event source, date, user, time stamp, source addresses, destination addresses, and other useful elements.	Election technology components – particularly servers and those devices in publicly accessible network interfaces – should capture detailed enough information to fully understand and reconstruct security incidents.	6.3

5.4 Incident Response and Management

CIS Control 19: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Election Technology Application

The fact that elections don't permit "do overs" should not dissuade anyone from planning and practicing an incident response plan. In fact, an effective and quickly executed incident response plan may protect the integrity of an election from even a sophisticated attack. The longer the attack goes on and the more ineffective the response, the higher likelihood the integrity of the election will be compromised. Election technology incident response plans should focus on early detection and response. Identifying the attack and its impact is one of the hardest challenges in incident response. Conducting tabletop exercises can help with this. The sooner you can identify an attack and its impact, the sooner you can isolate the impact and execute plans to remediate and recover. Remediation is possible in some cases but is not always possible in the limited time frame of an election. Therefore, part of an incident response plan must focus on backup options that can be deployed in the immediate aftermath of detecting an incident. This means having hot or warm backup options for nearly all critical systems.

In elections, as with most other domains, incident response is not done in a vacuum. It is critical to identify and communicate with your federal, state, local, and vendor partners when developing and testing your incident response plans.

5.4.1 Document Incident Response Procedures

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Ensure there are written incident response plans that define roles of personnel as well as phases of incident management.	Identify how to respond based on the type of incident and at what point during the election cycle the incident occurs. Incidents on Election Day will be treated differently than during a non-election time period.	19.1

5.4.2 Assign Job Titles and Duties for Incident Response

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.	At a minimum, identify which role is responsible for what and ensure each person in that role knows about their responsibility.	19.2

5.4.3 Designate Management Personnel to Support Incident Handling

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	When looking at possible incidents, identify organizational groups that will be impacted and ensure the organizational management is aware of their responsibility in the event of that type of incident. This might include an IT infrastructure manager, logistics manager, polling place coordinator, and others.	19.3

5.4.4 Devise Organization-wide Standards for Reporting Incidents

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	Early detection and response are key to ensuring that election integrity is maintained in the event of an incident. Permanent and temporary election staff (e.g., poll workers) should be trained on when and how to report potential incidents.	19.4

5.4.5 Maintain Contact Information for Reporting Security Incidents

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Assemble and maintain information on third-party contact information to be used to report a security incident, such as law enforcement, relevant government departments, vendors, and ISAC partners.	In the rush to respond to an incident, ensure someone is responsible for partner coordination. Do not task this to someone who will be asked to remediate the incident.	19.5

5.4.6 Publish Information Regarding Reporting Computer Anomalies and Incidents

Profile Applicability:	Description:	Notes:	CIS Control:
Level 1	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	All employees, including temporary election staff, should be trained on how to report possible suspicious activity.	19.6

5.4.7 Conduct Periodic Incident Scenario Sessions for Personnel

Profile Applicability:	Description:	Notes:	CIS Control:
Level 2	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to realworld threats. Exercises should test communication channels, decision-making, and incident responders' technical capabilities using tools and data available to them.	Exercises, such as the tabletop exercises, will challenge incident response plans and will ensure that the date of an incident is not the first time you are wrestling with tough questions.	19.7

5.4.8 Create Incident Scoring and Prioritization Schema

Profile Applicability:	Description:	Notes:	CIS Control:
Level 3	Create incident scoring and prioritization schema based on known or potential impact to your organization. Use the score to define frequency of status updates and escalation procedures.	Once an incident is identified and the scope of its impact is determined, it is not always necessary to have everyone involved with constant updates. Some incidents can be handled by a subset of personnel. Having an incident scoring system built into your incident response plan will help ensure a proportionate response.	19.8

Appendix A:
Secure Programming

A1.1 Data Protection

A1.1.1 Limit the Use and Storage of Sensitive Data

Profile Applicability:
Level 1

Description:
Conduct an evaluation to ensure that sensitive data is not being unnecessarily transported or stored. Where possible, use tokenization to reduce data exposure risks.

A1.1.2 Use Valid HTTPS Certificates From a Reputable Certificate Authority

Profile Applicability:
Level 1

Description:
HTTPS certificates should be signed by a reputable certificate authority (CA). The name on the certificate should match the fully qualified domain name (FQDN) of the website. The certificate itself should be valid and not expired.

A1.1.3 Disable Data Caching Using Cache Control Headers and Autocomplete

Profile Applicability:
Level 1

Description:
Browser data caching should be disabled using the cache control HTTP headers or meta tags within the hypertext markup language (HTML) page. Additionally, sensitive input fields, such as the login form, should have the autocomplete=off setting in the HTML form to instruct the browser not to cache the credentials.

A1.1.4 Set Up Secure Key Management Processes

Profile Applicability:
Level 1

Description:
When keys are stored in your system, they must be properly secured and only accessible to the appropriate staff on a need-to-know basis.

A1.1.5 Updated TLS Configuration on Servers

Profile Applicability:
Level 1

Description:
Weak ciphers must be disabled on all servers. For example, SSL v2, SSL v3, and TLS protocols prior to v1.2 have known weaknesses and are not considered secure. Additionally, disable the NULL, RC4, DES, and MD5 cipher suites. Ensure all key lengths are greater than 128 bits, use secure renegotiation, and disable compression.

A1.1.6 Use TLS Everywhere

Profile Applicability:
Level 1

Description:
TLS should be used whenever data is transferred over a network. TLS must be applied to any authentication pages as well as all pages after the user is authenticated. If sensitive information (e.g., personal information) can be submitted before authentication, those features must also be sent over TLS.

A1.1.7 Securely Exchange Encryption Keys

Profile Applicability:
Level 1

Description:
If encryption keys are exchanged or preset in your application, any key establishment or exchange must be performed over a secure channel.

A1.1.8 Store User Passwords Using a Strong, Iterative, Salted Hash

Profile Applicability:
Level 1

Description:
User passwords must be stored using secure hashing techniques with strong algorithms like PBKDF2, bcrypt, or SHA-512. Simply hashing the password a single time does not sufficiently protect the password. Use adaptive hashing (a work factor) combined with a randomly generated salt for each user to make the hash strong.

A1.1.9 Disable HTTP Access for All TLS-Enabled Resources

Profile Applicability:
Level 1

Description:
For all pages requiring protection by TLS, the same URL should not be accessible via the non-TLS channel.

A1.1.10 Use the Strict-Transport-Security Header

Profile Applicability:
Level 1

Description:
The Strict-Transport-Security header ensures that the browser does not talk to the server over non-TLS. This helps reduce the risk of TLS stripping attacks as implemented by the TLSsniff tool.

A1.2 Authentication

A1.2.1 Don’t Hardcode Credentials

Profile Applicability:
Level 1

Description:
Never allow credentials to be stored directly within the application code. While it can be convenient to test the application code with hardcoded credentials during development, this significantly increases risk and should be avoided.

A1.2.2 Develop a Strong Password Reset System

Profile Applicability:
Level 1

Description:
Password reset systems are often the weakest link in an application. These systems are often based on the user answering personal questions to establish their identity and in turn reset the password. Ideally, such systems will leverage other known authenticators, such as confirming possession of a hardware token or a mobile device. When you do ask questions for password resetting, base them on questions that are both hard to guess, hard to brute force, and are not available through social media or previous data breaches. Additionally, any password reset option must not reveal whether an account is valid, preventing username harvesting.

A1.2.3 Implement a Strong Password Policy

Profile Applicability:
Level 1

Description:
A password policy should be created and implemented so that passwords meet specific strength criteria.

A1.2.4 Implement Protections Against Brute Force Attacks

Profile Applicability:
Level 1

Description:
Account lockout needs to be implemented to guard against brute forcing attacks against both the authentication and password reset functionality. After several tries on a specific user account, the account should be locked for a period of time or until unlocked by an administrative action or use of a separate authenticator controlled by the user. Additionally, it is best to continue the same failure message indicating that the credentials are incorrect or the account is locked to prevent an attacker from harvesting usernames.

A1.2.5 Don't Disclose Too Much Information in Error Messages

Profile Applicability:
Level 1

Description:
Messages for authentication errors must be clear and, at the same time, must be written so that sensitive information about the system is not disclosed. For example, error messages that reveal that the userid is valid but that the corresponding password is incorrect confirms to an attacker that the account does exist on the system. Instead, provide only a message that indicates that the login failed.

A1.2.6 Store Database Credentials Securely

Profile Applicability:
Level 1

Description:
Modern web applications usually consist of multiple layers. The business logic tier (processing of information) often connects to the data tier (database). Connecting to the database, of course, requires authentication. The authentication credentials in the business logic tier must be stored in a centralized location that is locked down. Scattering credentials throughout the source code is not acceptable. Some development frameworks provide a centralized secure location for storing credentials to the backend database. These encrypted stores should be leveraged when possible.

A1.2.7 Applications and Middleware Should Run With Minimal Privileges

Profile Applicability:
Level 1

Description:
If an application becomes compromised, it is important that the application itself and any middleware services be configured to run with minimal privileges. For instance, while the application layer or business layer needs the ability to read and write data to the underlying database, administrative credentials that grant access to other databases or tables should not be provided.

A1.2.8 Provide Options for Multifactor Authentication

Profile Applicability:
Level 1

Description:
Allow users to protect their accounts with multifactor authentication. Allow users to choose the authenticator that works best for them, subject to meeting security requirements. Where possible, allow the issuance of multiple authenticators so that multiple combinations can still meet an MFA requirement and be used in the reissuance of lost or stolen authenticators.

A1.3 Input and Output Handling

A1.3.1 Use the X-Frame-Options Header

Profile Applicability:
Level 2

Description:
Use the X-Frame-Options header to prevent content from being loaded by a foreign site in a frame. This mitigates Clickjacking attacks. For older browsers that do not support this header, add frame busting JavaScript code to mitigate Clickjacking (although this method is not foolproof and can be circumvented).

A1.3.2 Use Secure HTTP Response Headers

Profile Applicability:
Level 1

Description:
To protect against cross-site scripting (XSS) and man-in-the-middle (MITM) attacks, use the Content Security Policy (CSP), X-XSS-Protection, and Public-Key-Pins headers.

A1.3.3 Use the Nosniff Header for Uploaded Content

Profile Applicability:
Level 2

Description:
When hosting user uploaded content that can be viewed by other users, use the X-Content-Type-Options: nosniff header so that browsers do not try to guess the data type. Sometimes the browser can be tricked into displaying the data type incorrectly (e.g., showing a GIF file as HTML). Always let the server or application determine the data type.

A1.3.4 Validate the Source of Input

Profile Applicability:
Level 2

Description:
The source of the input must be validated. For example, if input is expected from a POST request, do not accept the input variable from a GET request.

A1.3.5 Conduct Contextual Output Encoding

Profile Applicability:
Level 2

Description:
All output functions must contextually encode data before sending it to the user. Depending on where the output will end up in the HTML page, the output must be encoded differently. For example, data placed in the URL context must be encoded different than data placed in JavaScript context within the HTML page.

A1.3.6 Validate Uploaded Files

Profile Applicability:
Level 1

Description:
When accepting file uploads from the user, make sure to validate the size of the file, the file type, and the file contents as well as ensure that it is not possible to override the destination path for the file.

A1.3.7 Set the Encoding for Your Application

Profile Applicability:
Level 1

Description:
For every page in your application, set the encoding using HTTP headers or meta tags within HTML. This ensures that the encoding of the page is always defined and that the browser will not have to determine the encoding on its own. Setting a consistent encoding, like Unicode transformation format 8 bit (UTF-8), for your application reduces the overall risk of issues like XSS.

A1.3.8 Use Tokens to Prevent Forged Requests

Profile Applicability:
Level 1

Description:
In order to prevent Cross-Site Request Forgery (CSRF) attacks, you must embed a random value that is not known to third parties into the HTML form. This CSRF protection token must be unique to each request. This prevents a forged CSRF request from being submitted because the attacker does not know the value of the token.

A1.3.9 Use Parameterized SQL Queries

Profile Applicability:
Level 1

Description:
SQL queries should be crafted with user content passed into a bind variable. Queries written this way are safe against SQL injection attacks. SQL queries should not be created dynamically using string concatenation. Similarly, the SQL query string used in a bound or parameterized query should never be dynamically built from user input.

A1.3.10 Prefer Whitelists Over Blacklists for Input Validation

Profile Applicability:
Level 1

Description:
For each user input field, there should be validation on the input content. Whitelisting input is the preferred approach. Only accept data that meets certain criteria. For input that needs more flexibility, blacklisting can also be applied where known bad input patterns or characters are blocked.

A1.4 Access Control

A1.4.1 Apply the Principle of Least Privilege

Profile Applicability:
Level 1

Description:
Make use of a Mandatory Access Control system. All access decisions will be based on the principle of least privilege. If not explicitly allowed, access should be denied. Additionally, after an account is created, rights must be specifically added to that account to grant access to resources.

A1.4.2 Apply Access Controls Checks Consistently

Profile Applicability:
Level 1

Description:
Always apply the principle of complete mediation, forcing all requests through a common security gatekeeper. This ensures that access control checks are triggered whether or not the user is authenticated.

A1.4.3 Don't Use Unvalidated Forwards or Redirects

Profile Applicability:
Level 2

Description:
An unvalidated forward can allow an attacker to access private content without authentication. Unvalidated redirects allow an attacker to lure victims into visiting malicious sites. Prevent these from occurring by conducting the appropriate access control checks before sending the user to the given location.

A1.4.4 Don't Use Direct Object References for Access Control Checks

Profile Applicability:
Level 2

Description:
Do not allow direct references to files or parameters that can be manipulated to grant excessive access. Access control decisions must be based on the authenticated user identity and trusted server-side information.

A1.5 Session Management

A1.5.1 Set the Cookie Domain and Path Correctly

Profile Applicability:
Level 2

Description:
The cookie domain and path scope should be set to the most restrictive settings for your application. Any wildcard domain scoped cookie must have a good justification for its existence.

A1.5.2 Set the Cookie Expiration Time

Profile Applicability:
Level 1

Description:
The session cookie should have a reasonable expiration time. Non-expiring session cookies should only be allowed for applications with no sensitive information, such as one providing basic public information that is customized for a user.

A1.5.3 Place a Logout Button on Every Page

Profile Applicability:
Level 1

Description:
The logout button or logout link should be easily accessible to the user on every page after they have authenticated.

A1.5.4 Use Secure Cookie Attributes (HttpOnly and Secure Flags)

Profile Applicability:
Level 1

Description:
The session cookie should be set with both the HttpOnly and Secure flags. This ensures that the session ID will not be accessible to client-side scripts and it will only be transmitted over HTTPS.

A1.5.5 Ensure That Session Identifiers Are Sufficiently Random

Profile Applicability:
Level 1

Description:
Session tokens must be generated by secure random functions and must be at least 128 bits or provide 64 bits of entropy.

A1.5.6 Invalidate the Session After Logout

Profile Applicability:
Level 1

Description:
When the user logs out of the application, the session and corresponding data on the server must be destroyed. This ensures that the session cannot be accidentally revived.

A1.5.7 Destroy Sessions at Any Sign of Tampering

Profile Applicability:
Level 2

Description:
Unless the application requires multiple simultaneous sessions for a single user, implement features to detect session cloning attempts. Should any sign of session cloning be detected, the session should be destroyed, forcing the real user to reauthenticate.

A1.5.8 Implement an Absolute Session Timeout

Profile Applicability:
Level 3

Description:
Users should be logged out after an extensive amount of time (e.g., 4-8 hours) has passed since they logged in, regardless of activity. This helps mitigate the risk of an attacker using a hijacked session.

A1.5.9 Implement an Idle Session Timeout

Profile Applicability:
Level 1

Description:
When a user is not active, the application should automatically log the user out. Be aware that Ajax applications may make recurring calls to the application, effectively resetting the timeout counter automatically.

A1.5.10 Regenerate Session Tokens

Profile Applicability:
Level 2

Description:
Session tokens should be regenerated when the user authenticates to the application and when the user privilege level changes. Additionally, should the encryption status change, the session token should always be regenerated.

A1.6 Error Handling and Logging

A1.6.1 Display Generic Error Messages

Profile Applicability:
Level 1

Description:
Error messages should not reveal details about the internal state of the application. For example, file system path and stack information should not be exposed to the user through error messages.

A1.6.2 No Unhandled Exceptions

Profile Applicability:
Level 1

Description:
Given the languages and frameworks in use for web application development, never allow an unhandled exception to occur. Error handlers should be configured to handle unexpected errors and gracefully return controlled output to the user.

A1.6.3 Suppress Framework Generated Errors

Profile Applicability:
Level 2

Description:
Suppress default error messages in development framework or platform and replace them with customized error messages. Framework-generated messages may reveal sensitive information to the user.

A1.6.4 Log All Authentication Activities

Profile Applicability:
Level 1

Description:
Log all authentication activities, whether successful or not.

A1.6.5 Log All Privilege Changes

Profile Applicability:
Level 1

Description:
Log all activities or occasions where the user's privilege level changes.

A1.6.6 Log Administrative Activities

Profile Applicability:
Level 2

Description:
Log all administrative activities on the application or any of its components.

A1.6.7 Log Access to Sensitive Data

Profile Applicability:
Level 2

Description:
Log all access to sensitive data. This is particularly important for corporations that have to meet regulatory requirements like Health Insurance Portability and Accountability Act (HIPAA), PCI, or Sarbanes-Oxley Act (SOX).

A1.6.8 Do Not Log Inappropriate Data

Profile Applicability:
Level 1

Description:
While logging errors and auditing access is important, sensitive data should never be logged in an unencrypted form. For example, under HIPAA and PCI, it would be a violation to log sensitive data into the log itself unless the log is encrypted on the disk. Additionally, it can create a serious exposure point should the web application itself become compromised.

A1.6.9 Store Logs Securely

Profile Applicability:
Level 1

Description:
Logs should be stored and maintained appropriately to avoid information loss or tampering by an intruder. Log retention should also follow the retention policy set forth by the organization to meet regulatory requirements and provide enough information for forensic and incident response activities.

A1.6.10 Log User Activity

Profile Applicability:
Level 2

Description:
Logging user activity – login times, page views, data accessed, etc. – can greatly assist with understanding the impact of security incidents involving user accounts. This is especially important for administrators.

Notes:
Take care to not log information that would violate voter or ballot privacy.

Appendix B:

CIS Controls Descriptions

CIS Control 3: Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including attackers (to "weaponize," deploy an attack, exploit), vendors (to develop, deploy patches, signatures, and updates), and defenders (to assess risk, regression-test patches, install).

Organizations that do not scan for vulnerabilities and address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities and sometimes-uncertain side effects.

A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an organization or even across organizations, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and XCCDF.

Advanced vulnerability scanning tools can be configured with user credentials allowing authorized individuals to perform more comprehensive scans. To account for the varying patch cycles of each vendor, the frequency of scanning activities should increase as the diversity of an organization's systems increases. In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators.

CIS Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/ correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The misuse of administrative privileges is a primary method for attackers to spread inside a target system. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote-control software to find administrative passwords and other sensitive data.

Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment, and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track/report on/correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared toward ease-of-deployment and ease-ofuse— not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software—all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users; widely accepted configurations should be used. Configuration management requires analysis of potentially hundreds or thousands of options to make good choices. Settings must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network accessible services and client software.

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

CIS Control 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Malicious software is an integral and dangerous aspect of internet threats, as it is designed to attack your systems, your devices, and your data. It is fast-moving, fast-changing, and enters through any number of points like end-user devices, email attachments, webpages, cloud services, user actions, and removable media. Modern malware is designed to avoid defenses, and to attack or disable them. Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. The defenses must also be deployed at multiple points of attack to detect, stop the movement of, or control the execution of malicious software.

Anti-virus and endpoint security suites are the most common forms of malware defense. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system. Anti-virus applications look for signatures of known malware. To ensure anti-virus signatures are up to date, organizations are encouraged to use automation and the administrative features of enterprise endpoint security suites to verify that anti-virus, antispyware, and host-based IDS features are active on every managed system. They are also encouraged to run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Being able to block malicious applications is only part of this section. There is also a big focus on collecting the logs to help organizations understand what happened within their environment, and this includes ensuring that there is logging enabled for various command line tools, such as Microsoft® PowerShell® and Bash. As malicious actors continue to develop their methodologies, many are starting to take a “live off the land” approach to minimize the likelihood of being caught. Enabling logging will make it significantly easier for the organization to follow the events and understand what happened and how.

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit them with default user IDs and passwords or widely available exploitation code.

CIS Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use—not security. Open services and ports, default accounts (including service accounts) and passwords, support for older (vulnerable) protocols, and pre-installation of unneeded software are often easily exploited in their default state. Managing secure configurations for networking devices is a process that involves regularly re-evaluating both the configuration items and allowed traffic flows.

Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and never reviewed, leaving a potential vulnerability even when the exception is no longer applicable to business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time.

Attackers search for vulnerable default settings, and gaps or inconsistencies in rule sets for firewalls, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

CIS Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Attackers focus on exploiting systems they can reach across the internet, including directly internet-exposed systems and workstations and laptop computers that pull content from the internet through network boundaries. These attackers use configuration and architectural weaknesses found on perimeter systems, network devices, and internetaccessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another's, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multilayered, relying on firewalls, proxies, perimeter networks known as demilitarized zones (DMZs), and network-based intrusion-protection and intrusion-detection systems (IPSs and IDSs, respectively). It is critical to filter both inbound and outbound traffic.

Boundary lines between internal and external networks are diminishing due to increased interconnectivity within and between organizations and increased deployment of wireless technologies. While these blurring lines make it easier for attackers to bypass boundary systems, boundary defenses still mitigate risk by separating networks with different threat levels, sets of users, data, and levels of control. Effective multi-layered defenses of perimeter networks help minimize successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

CIS Control 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information..

Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques. As organizations continue their move toward cloud computing and mobile access, they must take proper care to limit and report on data exfiltration while also mitigating the effects of data compromise.

Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems or protected information. Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause reputational damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past few years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.

Organizations should understand its sensitive information, where it resides, and who needs access to it. To derive sensitivity levels, organizations should put together a list of the key types of data and the overall importance to the organization. They can use this analysis to create an overall data classification scheme for the organization. Organizations should define labels, such as “sensitive,” “confidential,” and “public” and classify their data according to those labels. Once the critical information has been identified, it can be further subdivided based on the impact it would have to the organization if it were compromised.

Once the sensitivity of the data has been identified, create a data inventory or mapping that identifies business applications and the servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels. If possible, firewalls need to control access to each segment.

Access to data should be based on job requirements and a need-to-know. Job requirements should be created for each user group to determine what information the group needs access to in order to perform its jobs. Based on the requirements, access should only be given to the data segments or servers that are needed for each job function. Detailed logging should be turned on for servers in order to track access and allow for security personnel to examine incidents in which data was improperly accessed.

CIS Control 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 and modify these critical assets based on an approved classification.

The principle of least privilege ensures that users only have access to the data that is relevant to their role and no more. This helps protect the confidentiality and integrity of the data. The loss of control over protected or sensitive data by organizations is a serious threat to operations and a potential threat to national security. While some data is leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when record-retention practices are ineffective or nonexistent.

The use of cryptography has become the standard in protecting the confidentiality and integrity of data. Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources; however, controls should also be in place to mitigate the threat of data exfiltration in the first place. Digitally signing data provides an additional level of assurance that if the signature is valid, the data has not been compromised, and it originated with the entity who applied the digital signature.

Organizations should ensure that products used within an enterprise implement well-known and vetted cryptographic algorithms, as identified by NIST. Re-evaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data.

CIS Control 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Wireless technologies have become extremely commonplace. In fact, many laptops and tablets are no longer being built with ethernet ports and are expected to run entirely from cellular or Wi-Fi connections. There are five types of digital wireless technologies: satellite, cellular, Wi-Fi, Bluetooth, and near-field communication (NFC). These technologies provide great flexibility and convenience in everyday computing.

- Cellular technology is most commonly associated with mobile telephones. A cellular network or mobile network is a wireless network distributed over land areas with cells each serviced by a transceiver, known as a cell site or base station. Each telephone communicates with a nearby transmitter, which changes as the device moves around.
- Wi-Fi, or 802.11, is a popular local area wireless technology that enables an electronic device to exchange data or connect to the internet using radio waves. Primary concerns with Wi-Fi are device authentication, rough access points, man-in-the- middle attacks, and information leakage.
- Bluetooth is a wireless technology that is used primarily to allow individual devices to communicate with each other over short distances. Multiple Bluetooth devices can be connected at once. The primary concerns with Bluetooth are device authentication and insecure pairing.

- Near-field communication is a set of standards that uses short-range radio signals to transmit information between two devices. It is very common in the mobile payment industry. The main concern with NFC is eavesdropping.

Wireless technologies such as Zigbee, P.25, and satellite are not included here due to no known instances of them being used in elections.

CIS Control 16: Account Monitoring and Control

Actively manage the lifecycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for security personnel watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for red team testing (but not deleted afterward) have often been misused in this way. Additionally, some malicious insiders or former employees have gained access to accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems.

Accounts must also be tracked very closely. Any account that is dormant must be disabled and removed from the system after a predetermined period. All active accounts must be traced back to authorized users of the system, and they should use MFA. Users must also be logged out of the system after a period of inactivity to minimize the possibility of an attacker using their system to extract information from the organization.

CIS Control 17: Implement a Security Awareness and Training Program

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Employees are the first line of defense in any good security program. In some sense, the phrase "You are only as strong as your weakest link" is very true in security. While we attempt to build defense in-depth, sometimes all it takes is one employee to unknowingly install a malicious program on their computer to lead to a major security breach. This is why it's important that all employees know the importance of, and have a basic awareness of, how to keep themselves and the company secure. This starts with a security awareness program.

Examples include:

- System developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system lifecycle).
- IT operations professionals (who may not recognize the security implications of IT artifacts and logs).
- End users (who may be susceptible to social engineering schemes such as phishing).
- Security analysts (who struggle to keep up with an explosion of new information).
- Executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational and mission risk, and lack proper data to make relevant investment decisions).

Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points.

No cyber defense approach can effectively address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

CIS Control 18: Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Software security cannot be achieved by a single practice, tool, heroic effort, or checklist. It is the result of a comprehensive secure software engineering process that spans all parts of development from early planning through end of life. It is a complex activity requiring a complete program encompassing enterprise-wide policy, technology, and the role of people. There are many resources to help develop a Secure Development Lifecycle (SDL), but there is no one-size-fits-all approach. The process must be firm in its approach to security but flexible enough in its application to accommodate variations in several factors, including different technologies and development methodologies in use and the risk profile of the applications in question.

An effective software security program for application software must address security throughout the entire lifecycle and embed security in as a natural part of establishing requirements, training, tools, and testing. Modern development cycles and methods do not allow for sequential approaches. Acceptance criteria should always include requirements that application vulnerability testing tools be run, and all known vulnerabilities be documented. It is safe to assume that software will not be perfect, and so a development program must plan upfront for bug reporting and remediation as an essential security function.

For software that is acquired (commercial, open-source, etc.), application security criteria should be part of the evaluation criteria, and efforts should be made to understand the source's software practices, testing, and error reporting and management. Whenever possible, suppliers should be required to show evidence that standard commercial software testing tools or services were used, and that no known vulnerabilities are present in the current version. The actions in this section provide specific, high-priority steps that can improve application security.
In addition, we recommend use of some of the excellent comprehensive resources dedicated to this topic:

- The Open Web Application Security Project (OWASP) – OWASP is an open community that creates and shares a rich collection of software tools and documentation on application security. https://www.owasp.org.
- Software Assurance Forum for Excellence in Code (SAFECode) – SAFECode creates and encourages broad industry adoption of proven software security, integrity, and authenticity practices. https://www.safecode.org/.

CIS Control 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyberattack against an enterprise is not "if" but "when." When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communication strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly creating irreversible impacts than would otherwise be possible were an effective incident response plan in place.

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies.

"Amazon Web Services" is a trademark of Amazon.com, Inc. or its affiliates in the United States and/or other countries."

"Google Cloud" is a trademark of Google LLC.

Notes: