MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

RECOMMENDED SECURITY CONTROLS FOR VOTER REGISTRATION

NOVEMBER 2019

MTR190584

MITRE REPORT

MITRE

Recommended Security Controls for Voter Registration Systems

Version 1.0

McLean, VA

Author(s): Carter Casey
Johann Thairu
Susie Heilman
Susan Prince
Brett Pleasant
Marc Schneider

November 2019

This page intentionally left blank.

Abstract

Voter registration systems are critical and highly interconnected components of most states' election infrastructures. This report is directed at technical members of state and local governments that maintain such systems. It recommends actionable security controls that can be applied to protect these systems. These controls apply to various components of voter registration systems, as well as existing connections to many external entities, including government organizations such as motor vehicle authorities and the Social Security Administration, and non-government third-party organizations. Securing and verifying the authenticity of data shared over these connections will be an important step toward protecting elections from outside influence.

This page intentionally left blank.

Executive Summary

A secure election ecosystem is critical to our democratic system, and voter information is a key component of that ecosystem. Protecting this information is of the upmost importance due to the potential for adversaries to disrupt the electoral process by deleting or manipulating voter information. As evidenced by the widespread attacks during the 2016 election cycle, in which numerous states were targeted for compromise by nation-state actors, voter registration databases are of particular interest to sophisticated adversaries and even attacks that do not change any information can be used to undermine confidence in U.S. institutions and the perceived legitimacy of election outcomes.

The MITRE Corporation has developed a series of actionable recommendations that are intended to provide specific guidance on securing voter registration systems, which can be used by technical members of state and local governments that maintain such systems. These recommendations extend security best practices to these systems and their associated databases and, when possible, offer clear examples of tools or applications that can be used to improve security controls, as well as identifying additional guidance for improving security.

Because each state has implemented its own system(s) independently, we have included a generalized architecture of a voter registration system with expanded focus on the specific components that are relevant to this topic: the voter registration database (VRDB), which stores voter information such as name, address, ID numbers, and other information; the frontend systems, which are interfaces used by election officials and for online voter portals; and the data transfer processes by which states meet the requirement to support registration via the motor vehicle authority and match information in the VRDB with information in other databases.

Below is an overview of the security control recommendations:

- **Secure External Communications:** Evaluate, protect, and authenticate communications with the external systems that share and validate voter information (such as motor vehicle authorities) to ensure that connections are secure and do not offer a point of entry for external attack.
- **Strengthen External and Internal Network Defenses:** Deploy network segmentation, additional firewall and intrusion detection layers, and email and web content filtering to detect and halt attacks made through network connections.
- **Enhance Access Management:** Implement role-based access, multifactor authentication, device access control, and centralized and federated identity management, and perform supply chain risk assessment.
- **Improve System Management and Monitoring:** Implement logging and vulnerability management to improve visibility. Perform regular audits to ensure validity of the database and compliance to policies and procedures, and to verify and validate file authenticity.
- **Facilitate Recovery:** Perform regular backups, frequent system audits, and institute clear recovery plans to mitigate damage to election systems.
- **Ensure Continuity of Operations:** Identify and test failover methodology to ensure that operations can continue if a system fails.

Potential future research from MITRE, described in brief at the end of this report, may explore non-technical aspects of election security. In particular, approaches to implementing coordinated vulnerability disclosure processes for elections and research into the impact of policy decisions on the resilience of election infrastructure are critical areas that could use more attention.

While the scope of this project is limited to voter registration systems and, primarily, their use before election day to register voters, it is important to note that voter registration systems are often not isolated from other components of election infrastructure such as election management systems and electronic poll books. This paper is not intended to be a comprehensive list of controls, and our recommendations can be applied to different architectures that share core components.

Table of Contents

List of Figures

This page intentionally left blank.

1 Background

The Help America Vote Act of 2002 (HAVA) required all states with voter registration to maintain a central, "computerized" list of registered voters that serves as its official record. The law did not specify any security requirements for these lists, however, which has led to widely divergent security controls implemented within each state, on top of equally divergent architectures. These lists, voter registration databases, represent a key component of election infrastructure that was the target of numerous dedicated attacks. The Senate Select Committee on Intelligence (SSCI) recently published a report[1] detailing numerous attempts by Russian intelligence to compromise voter registration databases before, during, and after the 2016 election; some were successful.

Because of this consistent attention from attackers attempting to undermine the integrity of elections, concrete security guidance for voter registration systems can help improve the security of one aspect of the elections infrastructure and ecosystem. This document will provide concise, actionable recommendations for security controls that can help mitigate some of the worst vulnerabilities that may allow attackers to damage election integrity through attacks on voter registration systems.

1.1 Audience

This document is intended for election or other state officials who directly lead technical teams. These individuals will have deep insight into the workings of election systems and will be able to identify the components of such systems to which the recommended security controls apply.

1.2 Scope

Voter registration systems can be complex and, as noted above, vary from state to state. The next section of this document describes the generalized voter registration system architecture on which our security control recommendations are based. In short, this document assumes voter registration systems with a top-down centralized architecture that do not rely on external "cloud" services; it does not discuss functionality present in "election management systems," which may also contain voter registration services, and does not detail mitigations for electronic poll books specifically.

1.3 Related Work

This report is one of several resources available to election officials and aims to complement the work of others in the field. The Belfer Center for Science and International Affairs has produced

[1] Report of the Senate Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts against Election Infrastructure with Additional Views: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

the "State and Local Election Cybersecurity Playbook"[2] detailing high-level guidance for organizational approaches to improving election security. The Center for Internet Security (CIS), which operates the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), has produced "A Handbook for Election Infrastructure Security"[3] that addresses elections infrastructure as a whole. The Open Source Election Technology (OSET) Foundation has published resources for more secure architectures in online voter registration systems[4] and is working toward the goal of distributing open source software – including potential components of voter registration systems – for use in elections. The Global Cyber Alliance (GCA) has made available a "Cybersecurity Toolkit for Elections,"[5] a set of tools for maintaining basic cybersecurity defenses and a resource that this paper will refer to periodically for practical recommendations. The Center for Election Innovation & Research has published a report specific to voter registration database security that provides some high-level security guidance based on results of a survey issued to states.[6] Finally, the National Institute of Standards and Technology (NIST) is a government body that has published numerous guides and standards for securing systems, to which this report will refer frequently.[7] NIST also manages the Technical Guidelines Development Committee, which advises the Election Assistance Commission on the Voluntary Voting System Guidelines.

[2] The State and Local Election Cybersecurity Playbook: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[3] A Handbook for Elections Infrastructure Security: https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

[4] Best Practices for Online Voter Registration Systems: https://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure-yss33:

[5] GCA Cybersecurity Toolkit for Elections: https://gcatoolkit.org/elections

[6] Center for Election Innovation & Research, "Voter Registration Database Security": https://electioninnovation.org/2018-vrdb-security

[7] NIST maintains a close partnership with MITRE and sponsors some MITRE work, but did not influence the creation or content of this document.

2 Assumed Architecture

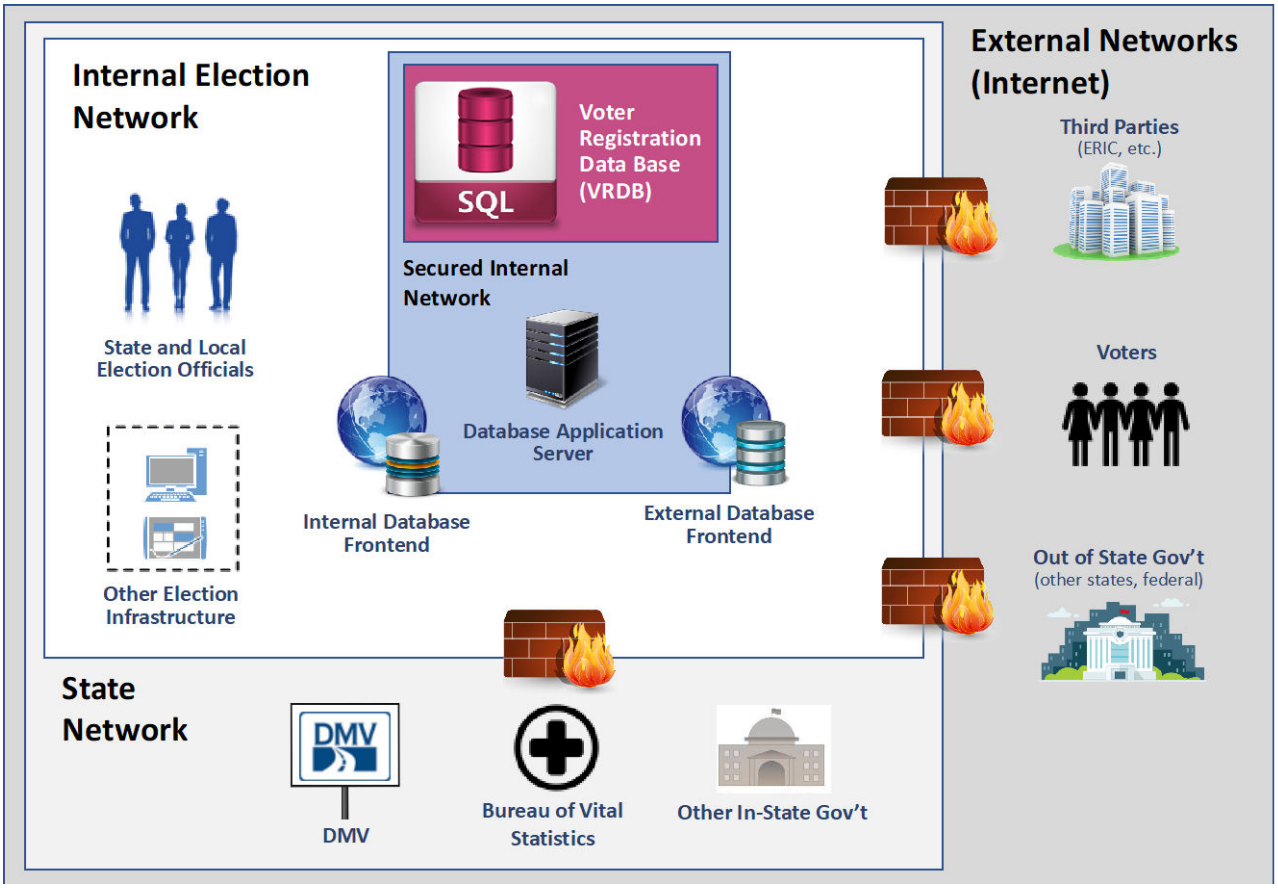

Figure 1. General Voter Registration System Architecture

Figure 1 above depicts a high-level overview of a generalized voter registration system architecture. The remaining subsections will expand on individual components within this diagram. Existing security measures are largely not included, as those may vary more broadly than the core components shown. The exceptions are simple firewalls (brick walls in the diagram above), which are placed at data transfer points to designate the perimeter of the state election system.

The architecture presented assumes that the system is based upon a three-tier model, divided into presentation, application, and persistence. The presentation layer consists of several different "frontend" components, which may be web based or thick client based. The diagram above assumes a public web-based interface for the frontend, which is represented as part of the external database frontend. The application layer consists of the database application server. The persistence layer consists of the voter registration database itself.

2.1 Architecture Description

2.1.1 Voter Registration Database

Figure 2. Voter Registration Database

The persistence layer and the heart of the system is the database itself. The database stores voter registration information, including names, addresses, ID numbers, and other information. There are a number of ways to implement a database, though most will involve well-structured storage maintained by a dedicated relational database application to provide for the properties of atomicity, consistency, isolation, and durability.

Though Figure 2 represents the database as a single item, the database will typically consist of multiple physical systems, including backup and replication, to improve performance and provide for high availability. This component also represents the entire database management system that administrators may use to perform various functions. The configuration and location of these systems, including whether they are co-located with the database application server (described below), will vary depending on the exact implementation. While the database may contain some business logic, such as stored functions, for the purposes of system decomposition, this logic is represented as belonging to the database application server.

2.1.1 Database Frontend Systems

The presentation layer is divided between two frontend systems, internal and external. While a typical implementation would likely include several different internally and externally facing user interface systems, they are represented here by two systems in order to simplify the diagram and explanation.

2.1.1.1 Internal Database Frontend for State Election Officials

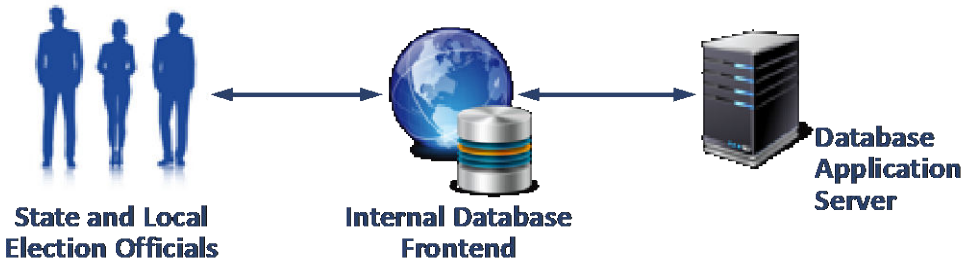

Figure 3. Internal Database Frontend

The internal frontend for the database is the primary interface used by election officials. It is designed to have finer grained, more privileged access to the database so that election officials can perform all required actions. For the same reasons, this component is likely to have stricter

access controls enforced via an internal identity and access management (IdAM) system (not shown in the diagram).

2.1.1.2 External Database Frontend

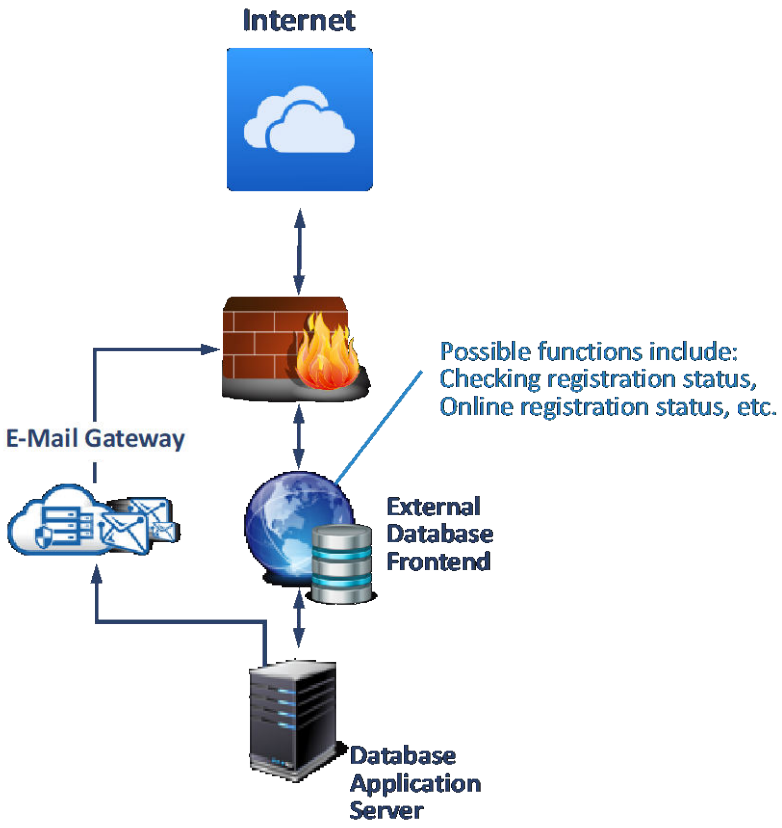

Figure 4. External Database Frontend

The external frontend for the database allows for several different use cases. The primary use case is for an online voter portal, which may include the ability to allow people to register to vote, check their voter registration status, or verify polling locations. Because this component is open to the public internet, its functionality is considerably reduced compared to that of the internal frontend, and there are likely a number of safeguards in place both prior to reaching the frontend application and within the application itself. An additional step of verification may be done before the data the voter submits is fully entered into the database, either within the database application or with the intervention of an election official.

An email gateway is included in this diagram to indicate that emails may be sent to the voter for the purposes of confirming their information, reminding them of important dates, and potentially other uses. It is not meant to be interactive, only sending emails out and not accepting them.

Secondary use cases for the external frontend include interfacing with other organizations when an interactive user interface is required.

2.1.2 Data Transfer

Data is transferred into and out of the voter registration system from various entities for the purpose of registering new voters and cross-checking existing or incoming registrations. These

entities include in-state government entities, out-of-state government entities, and third-party non-government entities.

2.1.2.1 Data Transfer from In-State Government Entities

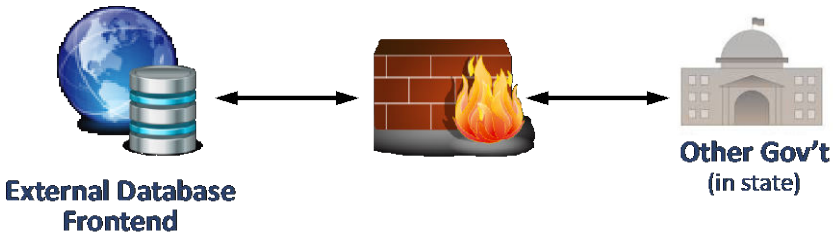

Figure 5. Data Transfer from In-State Government Entities

HAVA requires that state officials "match information in the database of the statewide voter registration system with information in the database of the motor vehicle authority," and the National Voter Registration Act of 1993 (NVRA) requires that each "driver's license application (including any renewal application) submitted to the appropriate State motor vehicle authority under State law shall serve as an application for voter registration." To exchange such information with the motor vehicle authority, and potentially other in-state entities including the authority on vital records, there is likely an interface for bulk data transfer to and from the database system. Figure 5 depicts the bulk data transfer of information from the other in-state government entities.

State government organizations may transfer data over a dedicated statewide infrastructure, if one is available, without passing through the public internet. Whether or not that occurs, these organizations will likely have their own security measures in place for all incoming, and ideally all outgoing, data.

Examples of In-State Government Entities

Below are some examples of agencies with which election officials commonly form agreements. It is not an authoritative list of all such organizations.

- The "motor vehicle authority" of the state, often the Department of Motor Vehicles (DMV). The state will likely receive voter registration information from this entity in accordance with federal law, as well as checking state-issued ID information while verifying voter registration.
- The state agency that records deaths, such as the Department of Health or Bureau of Vital Statistics. The state will use information from this entity to identify deceased voters and remove them from the rolls.
- Courts or state prison/corrections agencies, which provide conviction records in states that do not allow people convicted of certain crimes to vote.

2.1.2.2 Data Transfer from Out-of-State Government Entities

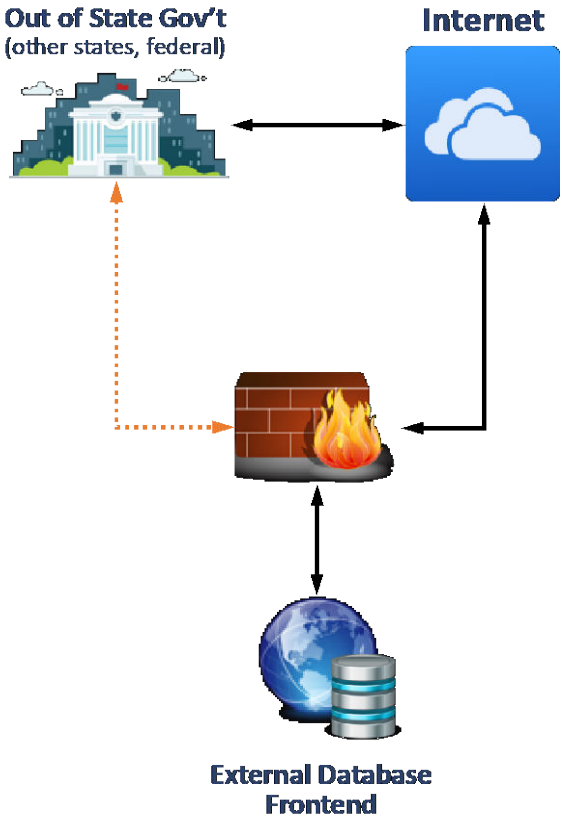

Figure 6. Data Transfer from Out-of-State Government Entities

Though HAVA requires only the motor vehicle authority to enter into an agreement with the Social Security Administration (SSA) for the purposes of verifying voter registrations, state election officials may still enter into their own agreements with the SSA and other federal or external state entities. As is the case with in-state organizations, these agreements could result in a dedicated interface separate from the usual internal or external frontend. However, it is much less likely that the state and these organizations will have access to a shared infrastructure over which data may be transferred, which would mean data is sent over the public internet. Figure 6 depicts the bulk data transfer of information from out-of-state and federal government entities.

Examples of Out-of-State Government Entities

Unlike the list of in-state entities that state election officials may interface with, the following list refers largely to federal agencies, or organizations within a specific state. That said, it should still not be considered authoritative.

- The SSA's Help America Vote Verification interface, which states can use to check the last four digits of a registrant's social security number.
- The United States Postal Service's National Change of Address Program, which can provide information to states when a resident reports to the program that they have moved.
- The Centers for Disease Control & Prevention's National Center of Health Statistics, which collects a variety of health information including vital statistics and can share death records with states in the event that residents die outside of the state's borders.

- Kansas' Interstate Voter Registration Crosscheck Program, through which states could share voter registration records. However, the program is under considerable scrutiny from various organizations including the American Civil Liberties Union and has not been run since 2017 due to security concerns[8].

2.1.2.3 Data Transfer from Third-Party Non-Government Entities

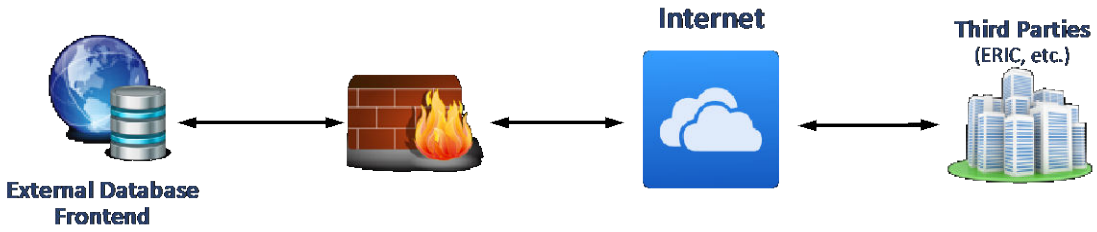

Figure 7. Data Transfer from Third-Party Non-Government Entities

A state may also enter into agreements with various non-government organizations, such as the Electronic Registration Information Center[9] (ERIC) and other groups that seek to coordinate or expand voter registration efforts. These groups, like government entities, may be given access to dedicated interfaces to share data with the voter registration system or vice versa. Figure 7 depicts the bulk data transfer of information from third-party non-government entities.

Even if they are located within a state, it is unlikely third parties will be able to use internal state infrastructure to transfer data, so data transfer with these third parties will likely occur over the public internet, and consequently be subject to stricter security controls.

Examples of Third-Party Non-Government Entities

As with previous sections, this is a short list of examples and should not be considered authoritative.

- ERIC allows participating states to share voter registration information, reducing duplicate registrations and otherwise increasing visibility between states.
- Rock the Vote[10] is an organization that runs a large number of voter registration drives, often using information obtained from voter registration systems, including from APIs provided by the state.
- Vote.org is a project aimed at simplifying voter registration across the United States, providing a very large number of interfaces to state online voter registration systems.

---

[8] Topeka Capital-Journal, "Kansas elections director: Crosscheck last used in 2017, when audit found security risks": https://www.cjonline.com/news/20190212/kansas-elections-director-crosscheck-last-used-in-2017-when-audit-found-security-risks

[9] ERIC: https://ericstates.org

[10] Rock the Vote: https://www.rockthevote.org

2.2 Architecture Scope

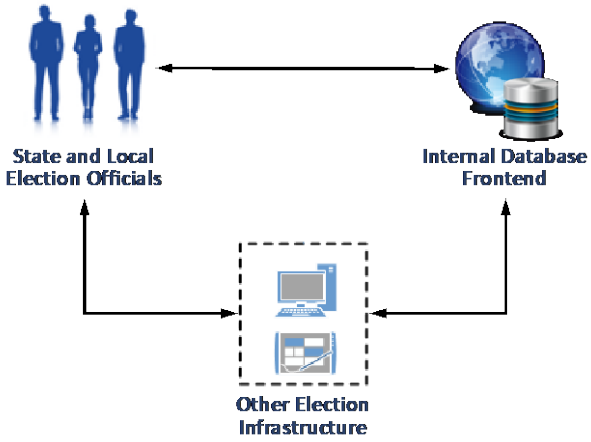

Figure 8. Additional Election Infrastructure

The scope of this project is limited to voter registration systems. However, voter registration systems are often not isolated from other components of election infrastructure. The component containing registration information may also include precinct mapping capabilities, and some systems may even include broader election management functionality such as absentee ballot management. Furthermore, a new trend in dedicated electronic poll books means that voter registration rolls may be downloaded for use in precincts, rather than being printed. The security of these systems or tools is not discussed in this paper, though the following sections describe them in greater detail.

2.2.1 Election Management Systems

Election management encompasses a broad set of tasks that election officials may need to complete in order to conduct elections. These include ballot layout and design, the mapping of precincts, and reporting election results, among many other potential tasks. Many election officials will include tasks related to voter registration in this category. Systems that support election management may also support voter registration, and even if the systems are not the same, a state's election management system (EMS) and voter registration system may be hosted in the same environment and otherwise interconnected.

Though these systems fall outside the scope of this project, an EMS presents additional attack surfaces that election officials should consider. The set of users that require access to an EMS may be larger than the set of users that require access only to the voter registration system, thus increasing opportunities for an attacker to gain access to the system. Connections between the EMS and voter registration system also present some risk: a compromised system can be used to access another system to which it is connected.

2.2.2 Electronic Poll Books

Electronic poll books, or e-poll books, are an electronic version of the paper voter rolls election officials use to check in voters when they arrive at their polling place. Instead of a large binder of voter registration information, e-poll books are typically tablets or computers that present the information in a simple application and help automate portions of the voter check-in process. Because these systems are electronic, the information they contain will be loaded from the voter registration system and can provide a potential attack vector. Some e-poll books may also expect

an uninterrupted connection over the internet to retrieve voter registration information, rather than storing the information locally; similarly, e-poll books may attempt to notify a central system when a voter has checked in. Again, though election day use of e-poll books falls outside the scope of this project, the flow of data between the voter registration system and the e-poll book is certainly of interest.

3 Recommended Security Controls

The controls below represent a best effort to identify actionable recommendations for election officials. In several cases, high-level recommendations are accompanied by examples of relevant tools or applications.[11] These examples are not meant as recommendations, and the unique circumstances of each office should drive the adoption of particular approaches. When providing examples is not practical, recommendations are coupled with descriptions of what tools and techniques must accomplish to be useful, or references to documents that provide detailed guidance on how best to implement controls or policies. Nothing presented here is meant to constitute an exhaustive list of controls, as such a list is likely impractical. All controls found in this document can be applied to many different architectures that share only core components, as specifying a single, unified security architecture would provide little value to the many different architectures across states.

3.1 Secure External Communications

Voter registration systems use a variety of connections to external systems with the goal of maintaining a more accurate and up-to-date list of registered voters. Whereas election systems have received increased scrutiny over the past few years, these external partners have not been so heavily scrutinized. Unfortunately, the privileged level of access that these external partners have, coupled with unsecured methods of data transfer (whether simple file transfer, email, or unencrypted web APIs) could make these partners key target as "pivot points" through which attackers might gain access to election systems. Some of the attacks documented in the SSCI report of Russian interference in U.S. elections can be better explained in this context, including attacks on a District Attorney's website and on the emails of a third-party registration organization.

These external partnerships may be legally required, and they can serve an important role in improving the accuracy of the voter registration database by detecting when voters have moved, providing additional channels through which prospective voters can register, etc. This section emphasizes key security controls that, while also applicable in other sections of the document, are especially critical for connections to external partner organizations.

3.1.1 Patterns of Communication

Election offices may partner with external entities in various ways, depending on the nature of the information they share. For instance, an election office may send periodic requests to pull data from the state's motor vehicle authority, while it receives data pushed periodically or in real time from the state's bureau of vital statistics. The way data is shared or requested will likely vary from state to state, and even from one partner to the next within the same state. It is unlikely that a particular connection pattern will affect the security of the voter registration system. It is, however, very important to understand and account for those patterns with respect to security controls applied to the system. Tying security controls as tightly as possible to particular practices helps close the gaps attackers could otherwise use to enter the system. Specific

[11] The Global Cyber Alliance (GCA) maintains a Cybersecurity Toolkit for Elections that provides recommendations for open tools that cover the basics of cybersecurity protection, a few of which are mentioned in this paper.

examples of how to accomplish tight application of security controls to communication practices will be provided in the relevant sections.

In addition to understanding the specific patterns of individual connections, it can be useful to establish overall baselines of network behavior. Using the monitoring capabilities discussed in Section 3.4, election officials should take samples of monitoring data that represent "business-as-usual" activity in the system. Multiple baselines will be necessary based on different timelines for the office: activity at midnight will likely be different from activity at noon, much as activity in the summer will likely be very different from that in the weeks before an election, especially if it is high profile. These baseline measurements can be used in several ways, such as input for anomaly detection tools, or for election officials to compare against in the event of suspected foul play. Note that changes to network architecture, including the addition, removal, or upgrading of components, can significantly alter expected baselines. This does not obsolete all previous baseline collections outright but should be a consideration when using those older measurements.

3.1.2 Protecting Connections

Encrypting connections helps protect data from being disclosed to or altered by attackers during transmission. Various forms of encryption are widely supported by modern hardware and software, to the point that enabling encryption is often as simple as updating an application's configuration. End-to-end encryption, through protocols such as TLS and SSH, protects data transferred between applications, and can be enabled for web and file transfer services directly. Network-layer encryption, such as that provided by IPSec VPNs, can provide additional protection by encrypting all network traffic that flows between the election office and external partners, as well as some internal network traffic. It can be enabled on most business networking hardware.

However, simply enabling encryption on a service does not ensure that it will be used, and some cipher suites are dangerously out-of-date. Data will be strongly encrypted only if *both* sides of a connection use up-to-date, compatible cipher suites. There are two potential failure modes if this is not the case. First, the two sides may fail to establish a connection, resulting in no data transferred. This "fail-safe" mode is preferable to the alternative: a connection is established with weak encryption – or none at all – resulting in an unsecured data transfer despite attempts to secure it.[12]

When configuring a service or device to use encryption, it is important to also *disable* unencrypted connections, as well as weak, deprecated cipher suites. Mozilla's "Server Side TLS" guide and the Open Web Application Security Project (OWASP) "TLS Cheat Sheet" provide guidance for end-to-end encryption, while NIST Special Publication (SP) 800-77[13] provides

[12] CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade'): https://cwe.mitre.org/data/definitions/757.html

[13] NIST SP 800-77, Guide to IPsec VPNs: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

guidance on implementing network-layer encryption through IPSec VPNs. NIST SP 800-57[14] provides thorough guidance regarding the management of cryptographic keys used in encryption.

3.1.3 Authenticating Endpoints

Election offices and their partners must ensure that when they exchange information, it comes from a legitimate source and is received at a legitimate destination. Encryption is only useful between trusted endpoints; without that trust, a malicious host can impersonate a legitimate host and establish an encrypted connection with the election office or vice versa. These man-in-the-middle attacks present a critical motivation for performing mutual authentication. As a connection is being established, the participants at both ends must prove that they are legitimately the entities they claim to be. Attackers are then unable to simply claim that they are a trusted endpoint and hijack or create a new, malicious connection. Typically, protocols that support strong encryption will support strong mutual authentication. The methods for each protocol vary, as do the types of certificates required to prove a service's, user's, or device's identity.

Additional mechanisms may be required to manage the certificates used in mutual authentication, especially sharing them between organizations. While state-run mechanisms may be helpful for performing mutual authentication between some agencies in the same state, additional mechanisms may be needed for authenticating out-of-state or other in-state external entities. Mutual authentication includes both authentication of end users communicating to machines and authentication of machines communicating to each other, referred to as machine-to-machine (M2M) authentication. Mutual authentication in M2M communications, such as periodic data transfers when no end user is involved, helps ensure each machine can be uniquely identified by a public key certificate. Since loss of this certificate can allow other systems to authenticate, it is recommended that hardware security modules be used for key generation, key storage, and cryptographic operations on systems participating in M2M communication. End user-to-machine authentication sharing and identity management across a variety of partners is discussed in Section 3.3.3.

3.1.4 Verifying Data

As much as mutually authenticated, encrypted connections can stop attackers from intercepting the data being transmitted between organizations, they are not enough to fully guarantee the integrity of that data. Verifying data after it has been sent, and in fact after it has been stored in any given location, requires a trusted digital signature of the data. A partner should sign any data being transferred to election officials using a certificate available to the election office; entities within the election office should also sign data whenever it is transferred or updated in the voter registration system. These signatures, available through most communication channels (including email) and in standard databases, can also help retain traceability of voter registration data. If every step of the data's path through the network and every related database transaction can be traced to a user or entity, it becomes much easier to determine if and where an error was introduced.

[14] NIST SP 800-57, Recommendations for Key Management: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

3.2 External and Internal Network Defenses

The interconnectedness of voter registration systems supports important functions, but in turn can introduce greater risk. Connections to the internet, to external partners through dedicated channels, and even between components of the election system itself can all provide opportunities for an attacker. Whereas other systems can be disconnected from networks without harming continued operations, voter registration systems cannot, and the approach to protecting the system is consequently more complex. By deliberately designing network connections and boundaries to be specific to the functions and criticality of each component, election officials can improve their ability to halt and detect attacks made through network connections.

3.2.1 Network Segmentation and Isolation

Whenever possible, unrelated components of the network should be segmented into separate, appropriately secured subsections. Any devices that connect directly to external networks, whether the internet or a dedicated network between organizations, should be strictly limited and placed in what is known as the perimeter network, or demilitarized zone (DMZ). Tools that support outward-facing network defenses, such as application gateways, proxies, intrusion detection systems, and other filters, should be kept in the DMZ between the external and internal networks, with firewalls separating the DMZ from other networks. While the networking ports of these tools must be exposed externally, their management and configuration ports should be secured and on a separate network. All network management should be conducted out of band using a separate, dedicated management network isolated from all other networks.

The internal network should also be segmented, further isolating the most critical components of the system. Determining which components are the most critical will depend on the jurisdiction. It is recommended that a formal process, such as business impact analysis[15], be used to determine the most critical components.[16] It is likely that the voter registration database and important security and high-access management tools should be in the most highly secured environment, whereas other tools and resources used for day-to-day tasks can be kept in a more accessible networked environment, and any employee's workstations will be separate from those in the least restricted section of the network. The voter registration database should not be accessible over the public internet. This means that any system, such as a web server, that is accessible over the public internet should not have direct access to the database system. Access to each increasingly secure segment of the network should be subject to more stringent access control, starting with re-authentication of users when they attempt to use a more restricted application. Some of the network defense tools that are placed in the DMZ should be replicated, with finer grained controls, between these internal networks. For instance, if it is deemed necessary that a user's workstation be capable of accessing the database, it should first pass through a fine-grained firewall and intrusion detection system to reach it. The principles of the Biba Integrity

[15] NIST SP 800-34, Contingency Planning Guide for Federal Information Systems: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[16] NIST, "Risk Management Framework Overview": https://csrc.nist.gov/Projects/risk-management/rmf-overview

Model,[17] which details how to design system architectures to protect data integrity, can be applied to network segmentation for this purpose.

3.2.2 Firewalls

Firewalls stop unwanted traffic from entering a network. How this is accomplished varies by where and how a firewall is configured. A strong security architecture may include several layers of firewall (or firewall functionality), each providing different types of protection. The first, most externally facing firewall should block all traffic except for that which is clearly identifiable as a pre-approved service or application. For instance, if a server's only approved function is secure web traffic, a firewall should allow only HTTPS traffic on inbound connections and block all other traffic, including any attempts to initiate an outbound connection. Additional layers of firewall may inspect additional aspects of incoming network packets; whether, for example, a request is attempting to delete a database record or to simply retrieve a web page. Understanding the nature of connections with external partners is important here; if the elections office only ever sends pull requests to the motor vehicle authority, that organization should never attempt to push data independently, and any requests to do so should be blocked.

Application-specific firewalls support even more detailed configuration and can inspect the data inside network transmissions, if a clear standard is available. A web application firewall configured for online voter registration could inspect the type of HTTP request being made and block any unexpected messages, such as DELETE or PUT requests. Work conducted through NIST aims to provide a clear standard for voter registration through a Common Data Format,[18] which could be used for filtering and analysis down to the individual voter registration transaction. Even simply verifying that data is in an appropriate format can help prevent data injection attacks, but further filtering can be deployed with greater knowledge of the materials involved.

The OSET Institute recommends the voter registration database be completely separated from the internet by an "Online Voter Registration Gateway."[19] The functionality of this gateway is similar to that of a "reverse" proxy used to separate any traffic from external networks from directly reaching sensitive internal components, such as the voter registration database. Firewalls inspect incoming requests to verify that they fit within accepted limits and parameters and determine whether they demonstrate any identified threat signatures. The reverse proxy then interprets the request and produces a new request that is sent to the sensitive component. The reverse proxy has a strictly limited set of parameters with which to produce requests and uses the bare minimum data from the external request, such that even if the incoming request contained unusual or unexpected parameters, they do not arrive at the underlying service.

---

[17] K Biba, "Integrity Considerations for Secure Computer Systems," MITRE Corporation, MTR-3153 (1975)

[18] NIST SP 1500-103: https://pages.nist.gov/VoterRecordsInterchange/

[19] Best Practices for Online Voter Registration Systems: https://www.osetfoundation.org/s/OSET_OVR-RefArchitecture_Feb18.pdf

3.2.3 Intrusion Detection Systems

Whereas firewalls typically inspect traffic for clearly defined values and parameters, an intrusion detection system (IDS) is deployed to inspect traffic for less obvious suspicious activity. The indicators detected by an IDS may include malware signatures, unusual traffic patterns, or alerts from other heuristics such as machine learning. Sometimes these tools are coupled with the ability to drop connections entirely based on such indicators, but given that they are less reliable, this can lead to problems if legitimate traffic is blocked. Machine learning-based indicators are especially susceptible to manipulation[20] if not monitored with human intervention. On the other hand, the alerts generated by an IDS can be useful to administrators, particularly at helping detect threats that have already gained access to internal networks. Monitoring traffic between lower and higher security network segments can also help detect attacks a firewall may be too rigid to block.

3.2.4 Device Access Control

All devices should be challenged for a valid and trusted machine certificate in order to join the election system network. The process of assigning, updating, and revoking machine certificates should be tied directly to inventory management, and only devices that have been explicitly approved and added to the inventory should be allowed on the network. NIST SP 800-133[21] and SP 800-57[22] provide guidance on generating and managing the cryptographic keys necessary for use with certificates.

Once authorized, each device will likely be assigned an IP address through DHCP. Monitoring the MAC/IP address pair for each authorized connection can provide a form of persistent access control, typically known as DHCP snooping, allowing the network access point to detect unauthorized devices taking advantage of an already authorized connection. If a new MAC address is detected in a packet with an IP address that has already been assigned to a device with a different MAC address, without a new DHCP exchange, it may indicate an intruder. Furthermore, the same approach may be used to detect if an authorized and critical system is *dis*connected from the network, an event that may warrant an alert to the relevant monitoring system. DHCP snooping can be enabled on most standard network devices capable of providing DHCP services. In networks where DHCP is not enabled, or if this approach is not desired or available, there are other network management tools, such as arpwatch[23], that can achieve similar goals.

3.2.5 Email, Web, and Content Filtering

Officials use their workstations for a variety of activities, including email and web browsing. While it may be most secure if a separate system is used for any access to sensitive components

---

[20] Paragraph: Thwarting Signature Learning by Training Maliciously: http://www0.cs.ucl.ac.uk/staff/B.Karp/paragraph-raid2006.pdf

[21] NIST SP 800-133, Recommendation for Cryptographic Key Generation: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r1.pdf

[22] NIST SP 800-57, Recommendation for Key Management: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[23] arpwatch(8): https://linux.die.net/man/8/arpwatch

of the election system, this may not always be practical. To reduce the vulnerability of users' workstations, administrators should use email and web content filtering to block internal devices (including privileged users' workstations) from accessing known malicious URLs or receiving email from known malicious addresses. Some tools will even "sanitize" emails to render any links or embedded scripts inert. Email filtering is especially useful in combating phishing attacks, in which individuals are sent emails with malicious contents or links that can allow attackers to recover sensitive information and even passwords. Web filtering can defend against "watering hole" attacks, in which an external website is compromised such that visiting the compromised website can extend the compromise to the system accessing it. Content filtering, typically done by examining traffic and downloaded files for signatures of known attacks, can provide additional mitigation against some forms of phishing attacks. The GCA recommends a number of tools[24] that can help build defenses against these forms of attack.

Common tools that are often used to improve quality of life while using email clients and web browsers can also provide useful security protections. Spam filtering can block malicious emails or even junk mail not designed to be critically malicious. Junk mail is often embedded with tracking and analysis software designed to gather information and send it back to ostensibly non-malicious actors. However, as this traffic is not subject to the same security controls as standard office communications, it is more susceptible to interception by malicious actors, who can then use it to mount future attacks. Ad blockers can have a similar impact. While ads are necessary for the financial stability of the current web ecosystem, they may also come embedded with tracking software and malware payloads. The GCA Toolkit resources mentioned in the previous paragraph[25] also detail tools for these purposes.

3.3 Access Management

Appropriate access to the voter registration system should be limited to preserve security, but never so much employees in the election office cannot do their jobs. Designing and managing employee access should be guided by the work employees are expected to do, closely fitting the systems they are authorized to access to the components they require to fulfill their roles. Access should also be based on the level of trust granted to individuals and incoming data, which is particularly relevant when deciding how to manage the ways external organizations can interact with the voter registration system. Untrusted organizations, or even those that have limited security controls in place, should be strictly limited in their access.

3.3.1 Role-Based Access

Access to different resources in a system should be restricted to the minimum that a user requires to complete their duties. Applying this concept, the principle of "least privilege," can prevent both accidental and malicious access errors, especially when driven by clearly defined tasks and roles within an organization. For example, though an employee may act as the database manager, they may not have official privileges to approve a new voter registration. A single user may perform multiple roles within a system, especially in small election offices; the database manager

[24] GCA Cybersecurity Toolkit for Elections: Prevent Phishing and Viruses: https://gcatoolkit.org/elections/prevent-phishing-and-viruses

[25] Ibid.

may also act as the system administrator, for instance. Nevertheless, they should actively switch between each role to accomplish particular aspects of their duties. This can be especially important in election systems, where the traceability of changes can help address and recover from breaches and other attacks. Understanding exactly who fulfills what role will reduce confusion that could arise if the access management system blocks a user from completing tasks, a frustration that could result in weakened adherence to the prescribed controls. NIST SP 800-53 provides methods and associated assessment procedures for ensuring that the principle of least privilege is implemented correctly.[26]

3.3.2 Multifactor Authentication

Strong passwords or passphrases are important to blocking basic attacks against the election system. However, the wisdom of the past decade that dictates "complexity" requirements for passwords has proven detrimental to improving security, often leading to insignificant improvements in strength at the expense of memorability and increases in password reuse[27]. Modern approaches to identity management, codified in the NIST SP 800-63 publications, recommend a broader but more manageable set of requirements for user authentication. Key among these is multifactor authentication, which requires a user to be authenticated with at least two of "(i) something you know (such as a password or PIN); (ii) something you have (such as a cryptographic identification device or a token); or (iii) something you are (such as biometric measurements)." [28] Requiring multiple sources of identity verification requires an attacker to obtain multiple pieces of information before gaining access to the system. While a user should probably still use a single (strong) password for their personal device or workstation, authenticating to networks, to devices over a network, and to critical applications (especially the voter registration database) should always be done using multifactor authentication.

Though certain notions of password complexity have proven counterproductive to security,[29] the strength of factors used in authentication remains a concern. Asking a user to produce longer passwords they find easy to remember is still important; one approach to accomplishing this is to allow and encourage "passphrases" that consist of multiple words, which can increase cryptographic complexity while not overly burdening memory. Offline password managers can securely store passwords for users and are especially beneficial for infrequently used passwords that are especially difficult to remember. "Something you have" factors are also a place for caution, particularly for election officials. Where sending tokens to a personal device like a phone may be reliable for authenticating individual consumers to a commercial product, this process may not be as secure for high-profile targets. With increased attention from nation-state actors, personal phones of election officials could be targeted with a number of remote attacks, including social engineering targeting both election officials and their service providers. For this

[26] NIST SP 800-53: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[27] See Appendix A, Strength of Memorized Secrets, of NIST SP 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management: https://pages.nist.gov/800-63-3/sp800-63b.html

[28] Multifactor Definition: https://csrc.nist.gov/glossary/term/Multi_Factor-Authentication

[29] NIST SP 900-63-3, Digital Identity Guidelines: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

reason, simple devices used to regularly generate random tokens, such as those compliant with FIDO Alliance standards,[30] are preferable, because they have no connection to the internet and are likely easier to protect.

3.3.3 Centralized and Federated Identity Management

The process and structure of identity management depends on the size and complexity of the organization. Given the technical systems present in election offices, they likely already maintain IdAM systems for office employees. There are many solutions for managing users' details and credentials, but all are contingent on the processes in place for managing employees more generally and will be unique to each office. For additional guidance on how to better manage and secure such systems, NIST has provided general guidance to the financial services sector in NIST SP 1800-9[31] and NIST SP 1800-18[32] that can be applied to election systems.

Sharing credentials *between* environments can be more complex, though there are standards – such as the Security Assertion Markup Language – for that purpose. Federated identity management[33] allows users in one organization's domain to access another entity's domain securely without having to go through multiple layers of access control. A process like this could provide election officials with a solution for interfacing with partners – as long as the partner is trusted to have implemented access management as securely as the election office. The advantage of federation is that users need to remember only one set of login credentials when accessing resources across multiple domains, though modern authentication and password managers (see Section 3.3.2) can help address this burden. The downside is that it creates a process by which outside organizations may access the election system without being individually approved in an access control system managed by election officials. This can introduce considerable risk if the outside organization does not have adequate controls in place, because attacks that would otherwise have to be directed at compromising accounts in the election office can instead be directed at one of multiple identity management systems or the means of federating those systems. When partnering with organizations in the same state, it may be preferable to instead rely on the state's IT management to provide shared access between systems, if such management is available to both parties.

3.3.4 Supply Chain Risk

As with most resources, this paper has so far presented access management in terms of users and their individual devices. To build a trustworthy system from the ground up, one must go further to understand the risks associated with every component that makes up that system. When

---

[30] FIDO Certified Products: https://fidoalliance.org/certification/fido-certified-products

[31] NIST SP 1800-9, Access Rights Management for the Financial Services Sector: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-arm-nist-sp1800-9-draft.pdf

[32] NIST SP 1800-18, Privileged Account Management for the Financial Services Sector: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-pam-nist-sp1800-18-draft.pdf

[33] NIST SP 800-63C, Digital Identity Guidelines Federation and Assertions: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

determining what hardware and software to deploy within their election system architecture, election officials should perform a risk assessment to determine what kind of data the component will have access to, the likelihood the component will be exploited, and the overall impact to the system if the component is successfully exploited. This risk assessment should also be expanded to cover components used by third-party providers with which the voter registration system interacts. NIST has performed several case studies[34] relating to supply chain risk that companies can build upon.

3.4 System Management and Monitoring

Election systems are often operated by small teams that have little time to spend reviewing every relevant data source within their system to detect problems. A variety of tools for monitoring and managing networks can help reduce the overhead required to do so. Visibility into and control over the voter registration system can help officials detect problems as they occur and respond to those problems promptly. Well-structured monitoring can identify malicious activity, dangerous misconfigurations, and unpatched vulnerabilities. It can also provide a traceable record within the system, which may prove to be an extremely important resource for forensic analysis after a known or suspected attack.

3.4.1 Logging, Aggregation, and Analysis

All communications with a secure system and activity within that system should be logged. This includes events such as reading or writing data to a database, creation of files by applications, machines within the system powering down, and many others. Logs will be produced by components of the system in which events actually occur, but they should be supplemented with additional monitoring tools that track overall activity within the system. For example, the EI-ISAC provides the Albert Intrusion Detection System to states, which produces valuable records of network activity. The GCA Elections Toolkit recommends basic logging and monitoring tools,[35] including the Albert System.

The information produced by logging may be extensive and difficult to store and process. Security information and event management (SIEM) tools aggregate and analyze these data flows to produce artifacts that security personnel use to detect and respond to vulnerabilities and attacks. A good SIEM tool is configurable to show relevant and useful information, reducing gigabytes of logs to a set of helpful, consumable indicators (and not to a screen full of indecipherable alarms all flashing red). It should also support updates to account for new threat intelligence, such as that which may be shared via an FBI FLASH, or through EI-ISAC.

Importantly, the process of transferring logs should always be done in a manner that preserves the security of the system from which the logs are produced. For instance, logs of events from a secure application should not be transferred out of that application via an unsecured connection, as that could allow an attacker to intercept data from high-security components without accessing those components. Consequently, tools that process logs from highly controlled components must also be highly controlled. The Biba Integrity Model lays out principles for

[34] Supply Chain Studies: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

[35] GCA Cybersecurity Toolkit for Elections: Log and Monitor: https://gcatoolkit.org/elections/log-and-monitor

designing a system architecture to protect data integrity. These principles apply broadly to securing voter registration systems.

3.4.2 Vulnerability Scanning

Vulnerability scanning tools help detect problems in the system before they can be exploited in an attack. Outdated operating systems, unpatched applications, unsecured network interfaces, and other vulnerabilities can be difficult to identify when they occur. Frequently scanning a system will identify these issues soon after they crop up, allowing officials to proactively patch software, replace components, or otherwise mitigate vulnerabilities. Importantly, attackers will use some of these same tools to scan their targets to find "low-hanging fruit" to exploit. Though they should have access to a much smaller surface area of election systems, it is important that officials know at least as much about the weaknesses in their systems as attackers could. Simple tools like nmap[36] help identify basic network vulnerabilities, including vulnerabilities that will be highly visible to an attacker. For more complete vulnerability scanning and testing, Kali Linux[37] provides a number of open tools – such as OpenVAS,[38] Zed Attack Proxy,[39] and Metasploit[40] – that IT staff can use for assessments.

3.4.3 Asset Management

Many scanning tools must be run against specific targets. "Rogue" devices and applications (those that are not approved or managed by network administrators) can be a persistent problem in networks with many components. These rogue devices and applications can themselves present a notable security risk, as any vulnerabilities in such components may go unmonitored and unpatched. Thorough inventory management can help identify rogue devices and can be aided by integrating with a networking auditing tool that identifies all devices in a network. A clear approval process that generates the contents of the system inventory is extremely important, as managing components added in a piecemeal fashion can lead to confusion and hidden problems. Approval should also be recurring, in which each system is audited to determine whether it still belongs on the network. Regularly "checking in" on the network goes a long way toward recognizing suspicious activity as it arises and being prepared to deal with it.

Even when system assets are approved and tested before being added to the network, they should be continuously monitored to verify their compliance with security policies. This could be accomplished, for example, by having agents running on these systems that periodically inventory all software on the system and make sure it is authorized and verify the configuration of approved applications. If unauthorized software or erroneous configuration is detected, an alert should be generated. Similarly, the agent can monitor configuration information and ensure

---

[36] GCA Cybersecurity Toolkit for Elections: Know What You Have: https://gcatoolkit.org/elections/know-what-you-have

[37] Kali Linux: https://www.kali.org

[38] Open Vulnerability Assessment Scanner: http://www.openvas.org

[39] Zed Attack Proxy: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

[40] Metasploit: https://www.metasploit.com

that the system software is up-to-date and has had the latest patches applied. A tool like OpenSCAP[41] can detect vulnerabilities published using the Security Content Automation Protocol (SCAP), such as the National Vulnerability Database[42] (NVD) published by NIST, and verify that systems meet organizational standards through predefined profiles, such as those published in Department of Defense Security Technical Implementation Guides.[43]

3.4.4 Patch Management

Up-to-date software will have the latest and most complete protections against vulnerabilities and threats. Implementing a comprehensive and strictly enforced patch management system across all devices in the elections environment is critical to security. Devices other than users' workstations should be patched through secure channels using automation, so that no one has to patch each system individually. Users' workstations should allow users to initiate patches but should also require that up-to-date patches be installed within a reasonable window. NIST SP 800-40[44] provides guidance on technologies that may be used for patch management in environments with a variety of networked devices. However, stability is critical in election systems; frequent or inopportune downtime from patches can cause a host of problems for officials. Patches should always be tested and reviewed before being distributed, and officials should develop clearly defined procedures for deciding when to apply patches. At the least, a well-structured decision-making process will take into account the time in the election cycle, laws that pertain to system updates, the interruptions that a patch may cause, the severity of any vulnerabilities that a patch may address, and what mitigations may be available if a patch cannot be applied. For the purposes of assessing the severity of vulnerabilities, officials should refer to the NVD, which includes standardized severity ratings for vulnerabilities calculated using the Common Vulnerability Scoring System[45,46] (CVSS).

3.4.5 Audits

Auditing is a critical part of security that involves the analysis of systems and practices within an organization in order to ensure that they conform to a predetermined standard.

3.4.5.1 Local Database Auditing

There are several techniques available for auditing databases, the most basic being manual auditing of individual transactions. This is likely not feasible for the scale at which voter registration systems are typically used. Event-driven audits are a more suitable technique, in which certain properties such as transaction types and user roles can be used to classify transactions that need to be audited. For these techniques to be effective, it is important to

---

[41] OpenSCAP: https://www.open-scap.org

[42] National Vulnerability Database: https://nvd.nist.gov

[43] Security Technical Implementation Guides: https://public.cyber.mil/stigs

[44] NIST SP 800-40, Guide to Enterprise Patch Management Technologies: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[45] NVD Vulnerability Metrics: CVSS: https://nvd.nist.gov/vuln-metrics/cvss

[46] Common Vulnerability Scoring System: https://www.first.org/cvss

maintain proper database logs as well as to group users appropriately with respect to the types of transaction they will perform. To perform log analysis, it is important that logs generated by all systems in the enterprise are aggregated at a single location, ideally through a SIEM tool, so that analysts can quickly and efficiently process this critical log information. Another auditing method would be random transaction auditing. In this method, auditors review random samples of different transactions, providing potentially broader, though less deterministic, coverage than event-driven audits. NIST SP 1800-11 details a reference architecture that employs these techniques.

3.4.5.2 Compliance Auditing

Security policies and procedures require upkeep, in part to ensure that they fit current best practices, but also to ensure that they are in place at all. Security compliance auditing can be applied both to components of the system and to users on that system. Compliance of technical components is determined through the configuration and settings of each device. For large networks, checking for compliance can be aided by automated configuration management. A tool is used to retrieve the configuration from each device, then compare this against a stored copy of the correct configuration. Such tools can also be used to push out standardized copies of the configuration across devices, reducing some of the burden and potential error that hand configuration entails. Users' workstations can also be monitored for compliance by software agents running on the workstations themselves, such as those used for asset management per the discussion in Section 3.4.3. The extent to which these agents inspect the device should be commensurate with the criticality of the work the device is used for, with workstations used to access highly secured components of the system receiving more stringent inspection.

Compliance auditing should also include routine readiness drills for employees to determine what policies and procedures are well understood. Employee audits should include interactive events that play out potential attacks or failures, also known as tabletop simulations.[47] It can also be informative to employ "red teaming," in which a group of trusted experts attempts to breach the system without employees being informed. These drills should also include scenarios in which recovery from disaster is necessary and as such should include practice in restoring systems to a healthy state from backups. For example, CALDERA[48] is an automated adversary emulation system built on the MITRE ATT&CK™ framework.[49] "CALDERA can be used to test endpoint security solutions and assess a network's security posture against the common post-compromise adversarial techniques contained in the ATT&CK model."[50] States can employ this tool within their red teaming auditing efforts not only to reduce the resources required for the tests, but also to test against specific attack methods to better access their voter registration systems' weaknesses. The goal of any of these events is to check whether employees are aware of the correct procedures. If they are not, the programs through which employees are educated about security procedures and prepared for events may need revision.

---

[47] Exercise Guide: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

[48] CALDERA: https://github.com/mitre/caldera

[49] MITRE ATT&CK framework: https://attack.mitre.org/

[50] https://www.mitre.org/research/technology-transfer/open-source-software/caldera

3.4.5.3 Automated File Integrity Checking Services

Automated file integrity checking services allow for verification and validation of file authenticity on systems. A typical file integrity checking service will utilize a local agent on each target system to scan all the local files and then create hash values for them. After the initial scan, the file integrity system will continuously scan for unauthorized changes. Once identified, the agent will report back to a centralized server where an administrator may take action.

3.4.6 Privileged Endpoint Security Services

Components of the system with privileged access, such as dedicated administrator workstations and servers that manage other system components, represent a high risk to the entire system if not monitored properly for threats. They will be the highest value targets for any attackers hoping to gain high-level access, and as a result they should be separated from other, less secure components of the system. Host intrusion detection services, anti-virus, and malware detection software are good defenses against security threats targeting privileged hosts.

3.5 Recovery

Security will always be an evolving science, and no matter how much work is done to harden a system against attacks, there will always be vulnerabilities. As election officials work to improve their defenses against attacks, they should also prepare to deal with any failures that do arise, whether unintentional or malicious, to ensure quick, stable, and complete recovery. Regular backups, frequent system audits, and clear recovery plans can dramatically mitigate damage to election systems, as well as maintain and even improve trust in those systems.

3.5.1 Recovery Strategy

Election officials are well acquainted with incident response plans, and they should use their expertise in that area to drive the development of technical backups and failovers. Such planning will dictate the critical components of the infrastructure that must be maintained during and after an incident. It is also critical to have audit trails from consistent system monitoring to determine what led to the incident. Determining the cause of the failure is important not only in understanding which systems and networks were affected but also in determining how the recovery process should be handled and helping to prevent similar incidents from happening in the future. To that end, it is crucial to have an incident response plan that includes a risk assessment of the architecture. This risk assessment will help to determine the critical components of the architecture as well as training that should be provided for members for the incidence response team.

3.5.2 Backups

Backups are an important part of incident recovery. To be properly executed and maintained, they require adequate planning as well as appropriate separation from the systems and networks for which they will be used. They must also support solutions that ensure the continued availability of data and services.

3.5.2.1 Data Retention

When deciding which kind of backup system to implement, an important factor that election officials should consider is their data retention policies. These policies can be dependent on the

federal,[51] state, and local laws in place at the time. As such, an important first step is to access the applicable policy with the longest retention rate and use that as the minimum baseline for determining how long to retain data. If no such policy exists, election officials should develop a detailed retention schedule that refers to specific types of voter registration data and how long each should be kept. Data should be retained long enough to fully recover from loss of data from the live system. Though various forms of backups may be put in place and may take longer to use for a full recovery, having *enough* to recover is crucial. Other important factors to consider include an assessment of the state's security/data integrity architecture. An assessment of the granularity available through current monitoring capabilities can be used to infer how long it will take to detect that there has been a problem, which can help determine how long the data retention policy should be.

3.5.2.2 Database Backup Methodology

When determining an appropriate backup plan, it is important to review the available hardware and the current retention policies in place. It is also important to consider the frequency of backups when determining which backup plan to implement, as increased frequency can improve recovery time with the trade-off of requiring more space. Various types of backups can be done, including full, incremental, and differential. Each has its own advantages and disadvantages, but, in general, states should employ a combination in order to ensure availability of data. Full backups include backing up all the files on the drive to a selected media destination. They have the advantage of having the fastest recovery time, with the trade-off of requiring the longest time to perform the actual backup. Incremental updates involve periodically backing up only the files that have changed since the previous backup. These are less time-consuming than a full backup but have a longer restoration time. Differential backups are similar to incremental backups, but they contain all of the data that has changed since the last full backup, making recovery faster than with incremental backups.

3.5.2.3 Transaction Log Backups

Transaction log backups are database specific. A transaction log contains all transactions that have been performed on a database since the log was last backed up or since the last full backup. By using this log, the system is able to restore the database to its previous state at any given time. This is an advantage over just using an incremental backup, which only allows restoration to one particular state. Furthermore, transactions should include an indication, preferably through a digital signature as discussed in Section 3.1.4, of what entity or user made the change. This can reinforce traceability in the system, making it much more straightforward to conduct forensic analysis after errors or attacks. It is important to keep the logs in fault-tolerant storage, as each portion of the log is required for the restoration process.

3.5.3 Continuity of Operations

Complete recovery after a failure may take time, and during that time failing system components will be unavailable. Preparations for a failure should include not only plans for a full recovery,

[51] 42 U.S.C. § 1974: https://www.govinfo.gov/app/details/USCODE-2010-title42/USCODE-2010-title42-chap20-subchapII-sec1974

but also for continuing to operate services deemed too essential to fail. The breadth of the services deemed essential will vary depending on individual policies and procedures and must be determined by election officials themselves. In general, minimizing the number of components from that must be replicated in a backup, or failover, system will reduce the cost and complexity of maintaining and using that failover system.

3.5.3.1 Failover Methodology

Failover refers to switching to a backup system in the event that a primary system fails. Failovers in the context of services that states might provide can come in two different states, cold or hot. A cold failover refers to a backup system that needs to be turned on or installed, whereas a hot failover refers to a backup system that is running in parallel with the main system and can be used immediately. An important first step when planning and implementing failover architecture is determining priorities in terms of availability of services and capabilities. For voter registration database security, these priorities might shift based on time. Closer to elections, services requiring access to a state's voter registration database might be deemed have a higher priority. As such, states may choose to have more frequent full backups closer to election days in order to shorten the recovery time of these essential services. States should aim to have hot failovers whenever they are deemed necessary to maintain the availability of data and services.

4 Potential Future Work in Policy-Driven Security

This paper recommends a number of technical security controls to help protect voter registration systems, many of which are tools that may be deployed simply by technical staff in an elections office. However, no tool will successfully protect a system without appropriate policies and procedures that guide the use of such tools. Backups afford little protection without procedures in place to recover from failures using those backups. Auditing that indicates an error in a voter's records must be coupled with policies that determine how to validate the records and correct data determined to be erroneous. This paper discusses such policies and procedures where necessary and, in some cases, recommends them as security controls in their own right.

In addition to the recommendations presented here, MITRE believes researching ways to improve the security of voter registration systems through higher level, policy-driven approaches is another essential step towards ensuring election integrity. Improved vulnerability disclosure procedures and the application of "software independence" to voter registration could be two critical areas of such research. The following sections provide some general background on the two subjects.

4.1 Vulnerability Disclosure and Management

Every system has vulnerabilities, no matter how many have been found or patched. No tool for detecting or mitigating vulnerabilities will find potential threats yet to be uncovered. The process of discovering new vulnerabilities, though it benefits from the help of automated systems, is complex and accomplished by security experts in various domains. The discovery of vulnerabilities in election systems is particularly reliant on experts dedicated to that subfield, as such systems are not broadly used outside election offices. Unfortunately, there are few open processes through which security researchers can properly disclose the vulnerabilities they find to officials. It would be a significant boon to election offices to institute a standard process through which researchers can work with officials to identify, catalog, monitor, and mitigate vulnerabilities as they arise.

An open process for reporting vulnerabilities would provide a channel through which valuable information for improving the security of election systems could be provided to election officials and researchers. Dedicated teams that discover vulnerabilities in election systems can help officials proactively address these vulnerabilities long before they are used for an attack, rather than being blindsided when a vulnerability becomes the vector for an attack.

Ensuring that the reporting process operates in both directions, with researchers communicating to election officials and election officials engaging with researchers, would also be impactful. Election officials have an intimate knowledge of what mitigations they can and cannot deploy (for instance, patching a system close to an election may not be feasible). Election officials also have contracts with election system vendors that they can use to help push reports of vulnerabilities back to the manufacturer. Researchers, using knowledge provided by officials, can gain additional insights and provide improved guidance on alternative mitigations or ways of monitoring for ongoing attacks. This cooperative process could be the best way to allow all vulnerabilities to be adequately addressed before a full disclosure of vulnerabilities is made public, retaining both technical security and trust in the elections process.

4.2 Software Independent Voter Registration

No matter how much is done to secure voter registration systems, it is impossible to ensure that no attacks will be successful. Defensive security will never be a perfect practice, and election offices with limited resources will remain poorly equipped to handle the attacks of a nation-state actor, especially if the attacks target systems outside the officials' control. In addition to implementing preventive security controls, officials should work to make elections more resilient to failures in election infrastructure and enable elections to recover from successful attacks.

Ron Rivest and John Wack have applied the principles of resiliency to voting machine software with the concept of "software independence."[52] They present the case that, due to the complexities of modern software, it is impossible to fully trust the integrity of something done solely in software. To combat this problem, they define software independence as follows:

> *A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome.*

They also make a distinction between weak and strong software independence. In weak software independence, an error may be detected, but it has an unrecoverable impact on the election. With strong software independence, the error is detected in such a way that it is possible to recover from it and preserve the integrity of the election.

Importantly, strong software independence necessitates policies that ensure the results of an election can be correctly recovered, because no technical solution could do so on its own. This is especially true when attempting to apply software independence to voter registration: with HAVA specifying that a "computerized list shall serve as the single system for storing and managing the official list of registered voters,"[53] it is difficult to separate the operations of the voter registration database from software. Instead, research of policies that rely on voter registration systems could provide considerable benefit. For example, the Congressional Research Service (CRS) has noted that registration deadlines may "inhibit a voter's ability to correct particular registration errors or altered data." [54] Though HAVA requires that election officials offer voters provisional ballots, it is not clear how to resolve an undetected attack that removes the records of an otherwise eligible voter after a deadline. For that matter, several aspects of adjudication vary widely between states, and some jurisdictions invalidate the entire ballot if cast in the wrong precinct.[55] This could leave voters susceptible to attacks that send them to the wrong polling place, especially in conjunction with a modified record in the database. Finally, large scale attacks or inaccuracies could cause delays in already resource-limited jurisdictions. As CRS notes that states "are often not equipped to use provisional ballots on a large scale," this could strain expected fallback methods. Approaches that address potential issues in these areas may help insulate election results from software-dependent systems.

---

[52] On the notion of "software-independence" in voting systems: https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[53] The Help America Vote Act of 2002: https://www.eac.gov/assets/1/6/HAVA41.PDF

[54] Congressional Research Service, "Election Security: Voter Registration System Policy Issues": https://crsreports.congress.gov/product/pdf/IF/IF11285

[55] National Conference of State Legislators, "Provisional Ballots": http://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx

5 Conclusion

Voter registration systems are a critical, highly exposed element of U.S. election infrastructure; the interconnectedness that eases the process of updating and maintaining registration can also present vulnerabilities. Certain baseline security practices will go a long way to protecting the integrity of these systems. By developing a thorough understanding of all external communication and using that understanding to implement strict, specific security controls, officials can reduce the risk that their systems can be breached through connections with trusted organizations. They can further reduce risks posed by both external and internal networking by segmenting their networks to restrict access to critical systems, and monitoring for and blocking any unauthorized attempts to access components of their infrastructure. Designing system access around the roles that employees perform and restricting that access using modern authentication practices can limit the extent to which employee's accounts can be exploited without hampering their work. Extensive monitoring and logging of system activity can be daunting for small offices but deploying management tools that ingest and simplify that information can allow administrators to detect attacks as they occur. Even if attacks have a tangible impact, election officials can extend their experience with incident recovery to develop backups of data and systems that will allow essential operations to continue as needed, and others to be recovered when possible.

The authors of this paper recognize that not all security is technical, and that some essential changes cannot be enacted in the election office alone. Improved channels for communicating vulnerabilities in election systems would bring officials valuable information and improve the speed and effectiveness of patches for those vulnerabilities. Implementing policies and procedures that make voter registration more flexible and responsive to voters could reduce the impact that interference with registration systems has on election results. None of these improvements, technical or otherwise, can be put in place overnight. In order to keep up with the steadily advancing world of technology and attacks against it, steady progress will require dedication and resources. It will also require a strong foundation on which to build; ideally, this report has provided the reader with a better understanding of what that starting point should be.

Appendix A NIST Cybersecurity Framework

The following table identifies correlations between the categories of the NIST Cybersecurity Framework and sections of this document, for improved reference.

Function	Category	Section in Report
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	❖ **3.3 Access Management** ➢ **3.3.1 Role Based-Access** ➢ **3.3.3 Device Access Control** ❖ **3.4 Management and Monitoring:** ➢ **3.4.3 Asset Management**
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	❖ **3.4 Management and Monitory** ➢ **3.4.3 Asset Management** ➢ **3.4.5 Audits** ❖ **4 Policy-Driven Security** ➢ **4.1 Vulnerability Disclosure and Management** ➢ **4.2 Software Independent Voter Registration**
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	❖ **3.5 Recovery**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	❖ **3.3 Access Management** ➢ **3.3.4 Supply Chain Risk** ❖ **3.4 System Management and Monitoring** ➢ **3.4.3 Asset Management** ➢ **3.4.4 Patch Management** ➢ **3.4.5 Audits**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	❖ **3.3 Access Management** ➢ **3.3.4 Supply Chain Risk** ❖ **3.4 System Management and Monitoring** ➢ **3.4.3 Asset Management** ➢ **3.4.4 Patch Management** ➢ **3.4.5 Audits**
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	❖ **3.4 Access Management** ➢ **3.3.4 Supply Chain Risk**

PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	❖ **3.1 Security External Connections** ➢ **3.1.3 Authenticating Endpoints** ➢ **3.1.4 Verifying Data** ❖ **3.3 Access Management** ➢ **3.3.1 Role-Based Access** ➢ **3.3.2 Multifactor Authentication** ➢ **3.3.3 Device Access Control** ➢ **3.3.5 Centralized and Federated Identity Management**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	❖ **3.4 System Management and Monitoring** ➢ **3.4.4 Audits** ▪ **3.4.4.2 Compliance Auditing**
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	❖ **3.5 Recovery** ❖ **3.4 Management and Monitory** ➢ **3.4.4. Audits** ▪ **3.4.4.3 Automated File Integrity Checking Services**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	❖ **3.3 Access Management** ➢ **3.3.1 Role-Based Access** ❖ **3.4 System Management and Monitoring**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	❖ **3.4 System Management and Monitoring:** ➢ **3.4.3 Asset Management**
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	❖ **3.2 External and Internal Network Defenses** ❖ **3.4 Management and Monitoring** ➢ **3.4.2 Vulnerability Scanning** ➢ **3.4.6 Privileged Endpoint Security Services**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	❖ **3.2 External and Internal Network Defenses** ➢ **3.2.3 Intrusion Detection Systems**
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	❖ **3.2 External and Internal Network Defenses** ➢ **3.2.3 Intrusion Detection Systems** ❖ **3.4 System Management and Monitoring** ➢ **3.4.1 Logging, Aggregation and Analysis** ➢ **3.4.2 Vulnerability Scanning**

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	❖ **3.2 External and Internal Network Defenses** ➢ **3.2.3 Intrusion Detection Systems** ❖ **3.4 System Management and Monitoring** ➢ **3.4.5 Audits**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	❖ **3.5 Recovery**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	❖ **3.5 Recovery**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	❖ **3.5 Recovery** ❖ **3.4 System Management and Monitoring** ➢ **3.4.5 Audits**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	❖ **3.5 Recovery**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	❖ **3.5 Recovery**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	❖ **3.5 Recovery**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	❖ **3.5 Recovery**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	❖ **3.5 Recovery** ❖ **4. Policy-Driven Security** ➢ **4.1 Vulnerability Disclosure and Management**

Appendix B Belfer Center State and Local Playbook

This table identifies specific sections of this paper that support the recommendations made by the Belfer Center for securing voter registration systems. The technical aspects of the Belfer Center recommendations are bolded, as these are the aspects primarily addressed in this report.

Recommendation	Section in Report
Patch and update all computers and servers that connect to the database.	❖ **3.4 Management and Monitoring** ➢ **3.4.2 Vulnerability Scanning** ➢ **3.4.3 Asset Management**
Ensure the database server is not accessible over the public internet. Restrict which external systems can write directly to the database.	❖ **3.2 External and Internal Network Defenses** ➢ **3.2.1 Network Segmentation and Isolation** ➢ **3.2.2 Firewalls**
Establish a baseline for normal data activity (new entries and edits to existing entries). Monitor actively against this baseline and investigate anomalies. Add human review for data changes—at a minimum, review weekly change summaries; ideally have an official review for automated updates.	❖ **3.1 Secure External Communications** ➢ **3.1.1 Patterns of Communication** ❖ **3.4 Management and Monitoring** ➢ **3.4.4 Audits**
Limit access to only those who need it. For those with access, restrict access to only their area of responsibility (e.g., a county official can only edit files for his/her county but may have read access to others). Regularly adjust access and permissions as personnel change.	❖ **3.3 Access Management**
Require two-factor authentication for anyone to log into the database— no exceptions.	❖ **3.3 Access Management** ➢ **3.3.2 Multifactor Authentication**
Make frequent backups of the VRDB. Conduct routine recover drills to ensure they work.	❖ **3.5 Recovery** ➢ **3.5.1 Backups** ❖ **3.4 Management and Monitoring** ➢ **3.4.4 Audits**
Do NOT allow web servers to connect directly to the VRDB.	❖ **3.2 External and Internal Network Defenses** ➢ **3.2.1 Network Segmentation and Isolation**
Have mechanisms in place to mitigate distributed denial of service attacks on the voter registration website.	❖ **3.5 Recovery** ➢ **3.5.3 Failover Methodology**

Appendix C Abbreviations and Acronyms

API	Application Programming Interface
CIS	Center for Internet Security
CVSS	Common Vulnerability Scoring System
DHCP	Dynamic Host Configuration Protocol
DMV	Department of Motor Vehicles
DMZ	Demilitarized Zone
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
EMS	Election Management System
ERIC	Electronic Registration Information Center
GCA	Global Cyber Alliance
GCA	Global Cyber Alliance
HAVA	Help America Vote Act of 2002
HTTPS	Hypertext Transfer Protocol Secure
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
MAC	Media Access Control
M2M	Machine-to-Machine Authentication
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSET	Open Source Election Technology
OVR	Online Voter Registration

OWASP	Open Web Application Security Project
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SP	Special Publication
SSA	Social Security Administration
SSCI	Senate Select Committee on Intelligence
TLS	Transport Layer Security
VPN	Virtual Private Network
VRBD	Voter Registration Database