The State and Local Election Cybersecurity Playbook

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY

FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Figure Illustrations by Jordan D'Amato

Cover photo: Voting machines in Miami Shores, Fla., Nov. 8, 2016, (AP Photo/Lynne Sladky)

The State and Local Election Cybersecurity Playbook

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber attacks and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair. Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals. Now, in February 2018, we are releasing a set of three guides designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is The State and Local Election Cybersecurity Playbook.

D3P is a bipartisan team of cybersecurity, political, and policy experts from the public and private sectors. To better understand both the cybersecurity and other challenges that elections face, our team of nearly three dozen professionals spent six months researching state and local election processes. We visited with 34 state and local election offices, observed the November 2017 elections in three states, and interviewed leading academic experts, election equipment manufacturers, and representatives of federal government agencies. We conducted a nationwide security survey with 37 participating states and territories, which identified detailed nuances in election processes and their corresponding risk considerations. We hosted two state election cybersecurity conferences where we engaged state and local election officials in "tabletop exercise" election simulations to increase awareness of the cybersecurity threats they face and improve their ability to mitigate those threats.

This research taught us many things. Most importantly, we learned how difficult it is to defend the multifaceted nature of the elections process. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique. We were humbled by the intricacies of election operations in each state we visited, and inspired by election officials' incredible level of commitment to the democratic process. We also learned that the leadership of election officials is critical in creating a more secure system. Secretaries of state, election board members, state election directors, and local election administrators set the tone—it's ultimately their job to create a culture in which all staff make security a top priority.

This Playbook is intended for leaders at every level who play a role in running elections. While the future threats elections face are multifaceted, one principle stands clear: defending democracy depends on proactive leadership. This Playbook focuses on the U.S. experience, but it is also relevant to election officials around the world facing similar threats. We have designed it to identify risks and offer actionable solutions that will empower state and local election officials to protect democracy from those who seek to do it harm.

Finally, we would like to thank the election officials around the country for whom we wrote this guide. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

AUTHORS

Meredith Berger, D3P, Harvard Kennedy School

Charles Chretien, Software Engineer, Jigsaw (Alphabet)

Caitlin Conley, Executive Director, D3P

Jordan D'Amato, D3P, Harvard Kennedy School

Meredith Davis Tavera, D3P, Harvard Kennedy School

Corinna Fehst, D3P, Harvard Kennedy School

Josh Feinblum, Chief Security Officer, DigitalOcean

Kunal Kothari, D3P, Harvard Kennedy School

Alexander Krey, D3P, Harvard Kennedy School

Richard Kuzma, D3P, Harvard Kennedy School

Ryan Macias, Election Assistance Commission

Katherine Mansted, D3P, Harvard Kennedy School

Henry Miller, D3P, Brown University

Jennifer Nam, D3P, Harvard Kennedy School

Zara Perumal, D3P, Massachusetts Institute of Technology

Jonathan Pevarnek, Software Engineer, Jigsaw (Alphabet)

Anu Saha, D3P, Massachusetts Institute of Technology

Mike Specter, D3P, Massachusetts Institute of Technology

Sarah Starr, D3P, Harvard Kennedy School

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Drew Bagley, Sr. Privacy Counsel & Director of Global Cyber Policy,
CrowdStrike

Daniel Bartlett, D3P, Harvard Kennedy School

Judd Choate, Colorado Election Director and President, National
Association of State Election Directors

Amy Cohen, Exec. Director, National Association of State Election Directors

Mari Dugas, Project Coordinator, D3P

Alan Farley, Administrator, Rutherford County, Tenn. Election Commission

David Forscey, Policy Analyst, National Governors Association

Robert Giles, Director, New Jersey Division of Elections

Mike Gillen, D3P, Harvard Kennedy School

Chad Hansen, Senior Software Engineer, Jigsaw (Alphabet)

Eben Kaplan, Principal Consultant, CrowdStrike

Matt Masterson, Commissioner, Election Assistance Commission

Sean McCloskey, Election Task Force, Department of Homeland Security

Amber McReynolds, Director of Elections, City and County of Denver, Colo.

Joel Mehler, Senior Consultant, CrowdStrike

Robby Mook, Co-Director, D3P

Rachel Neasham, D3P, LoLa

Daniel Perumal, D3P

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

John Sarapata, Head of Engineering, Jigsaw (Alphabet)

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Johanna Shelton, Director, Public Policy, Google LLC

Charles Stewart III, Professor, MIT

Michelle K. Tassinari, Director/Legal Counsel, Elections Division, Office
of the Secretary of the Commonwealth of Massachusetts

Frank White, Independent Communications Consultant

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager,
Belfer Center

Andrew Facini, Publications and Design Coordinator,
Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

The Playbook Approach

Election officials are democracy's frontline defenders. Our election system faces an array of threats designed to undermine vote integrity and public trust in the election process. It is crucial that everyone involved in the election process—from top-level leaders, like Secretaries of State and Election Administrators, to day-to-day operators, like clerks and election site workers—understand their role in protecting the process and the threats that it faces. To this end, this Playbook has two goals: (1) to make the most likely and most serious cybersecurity and information operation threats understandable to everyone involved in the election process; and (2) to offer state and local election officials basic risk-mitigation strategies to counter these threats.

Our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals, but implementation of some strategies will require their involvement. We also did not address every issue or policy challenge that impedes cybersecurity readiness. Instead, we focused on the vulnerabilities and threats that align to create risk to our election process.

Finally, we understand that election officials already face many challenges in delivering accessible, accurate and secure elections—not least of which are constraints on financial and staffing resources. This Playbook is written with those realities in mind.

We hope this guide will give election officials more confidence in deciding how to approach security strategies and a greater common understanding in working with the technical specialists needed to implement these strategies.

This Playbook consists of three parts:

Background: frames the elections operating environment.

Common Ground: provides 10 best practice principles applicable to every election jurisdiction and a list of research security insights by election system.

Technical Recommendations: offers basic risk-mitigation recommendations specific to five components of the election system: voter registration databases, vote casting, vote tallying, election night reporting, and internal and public communications.

Our appendices offer more specific recommendations on two complex topics: vendor selection and maintenance, and election auditing. Additionally, the D3P Team has put together two additional resources to help navigate the challenges of maintaining and preserving public trust: "The Election Cyber Incident Communications Coordination Guide" and "The Election Cyber Incident Communications Plan Template for State and Local Election Officials."

Introduction

Running elections is complicated. It requires year-round preparation and coordination. Election officials have a lot to manage to ensure that the process remains free, fair, and accessible. Historically, efforts to protect the election system have focused on physical security, but today's digital world requires that we also focus on cybersecurity and information operations to defend against malicious actors of varying motives and means.

Cyber Attack: an attack targeting a network for the purpose of disrupting, disabling, destroying, or maliciously controlling it; or an attempt to destroy the integrity of data or steal controlled information. Common attacks include: spear phishing (to gain unauthorized access to existing accounts), denial of service (DoS), and device takeover.

Information Operations: the dissemination of information, true or false, to manipulate public opinion and/or influence behavior. Digital technologies like social media have made it possible for nation-states to organize information operations at an unprecedented scale. Because the tools needed for information operations are incredibly cheap and widely accessible (all you need is access to the Internet), adversaries use information operations to gain an asymmetric advantage over the U.S. and compete for influence in the world. Common information operation tactics include: spreading fake or misleading information online, leaking stolen information online, and using social media to amplify opposing views and stir political conflict.

Cyber attack and information operations tactics are often used in coordination. For example, a malicious actor might hack an election official's email account, alter emails, and then use those stolen, altered emails to spread misinformation online. Alternatively, social media login credentials might be stolen, and an official account then used to create confusion.

Background

What's at Stake

A core tenet of democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it wasn't in reality.

The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. While it didn't affect the outcome of the election, it did reveal significant vulnerabilities in our elections process. The 2016 case was not the first time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections, including the upcoming November 2018 midterm elections. While these foreign operations are traditionally a matter for the intelligence community and federal law enforcement, responsibility to secure elections ultimately falls on local and state officials.

Cybersecurity Threats to Elections

U.S. elections are decentralized. The federal government provides national-level guidance, but state and local governments administer elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters.

The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and

experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.

The "Who" Behind Cyber Attacks & Information Operations Targeting Elections

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.

See the table on page 10 for an overview of known hostile actors.

KNOWN HOSTILE ACTORS THAT COULD TARGET U.S. ELECTIONS

Russia: The Department of Homeland Security, the U.S. intelligence community, CrowdStrike, and other private sector firms implicated Russian intelligence groups "Fancy Bear" and "Cozy Bear" in the 2016 U.S. presidential campaign hacks. Russian meddlers also probed information systems related to voter registration in 21 states, gaining access to at least two systems. Media sources also reported Russian hackers allegedly penetrated a U.S. election software vendor, hoping to gain information for a subsequent spear-phishing campaign against state and county election officials. In the run-up to (as well as since) the 2016 election, Russian-affiliated groups have conducted information operations using social media sites, exploiting existing fissures in American society. Similar coordinated efforts combining cyber attacks and information operations attempted to influence the 2014 Ukrainian and 2017 French elections.

China: In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials, or attempted to interfere with state election systems.

Iran: In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. If geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

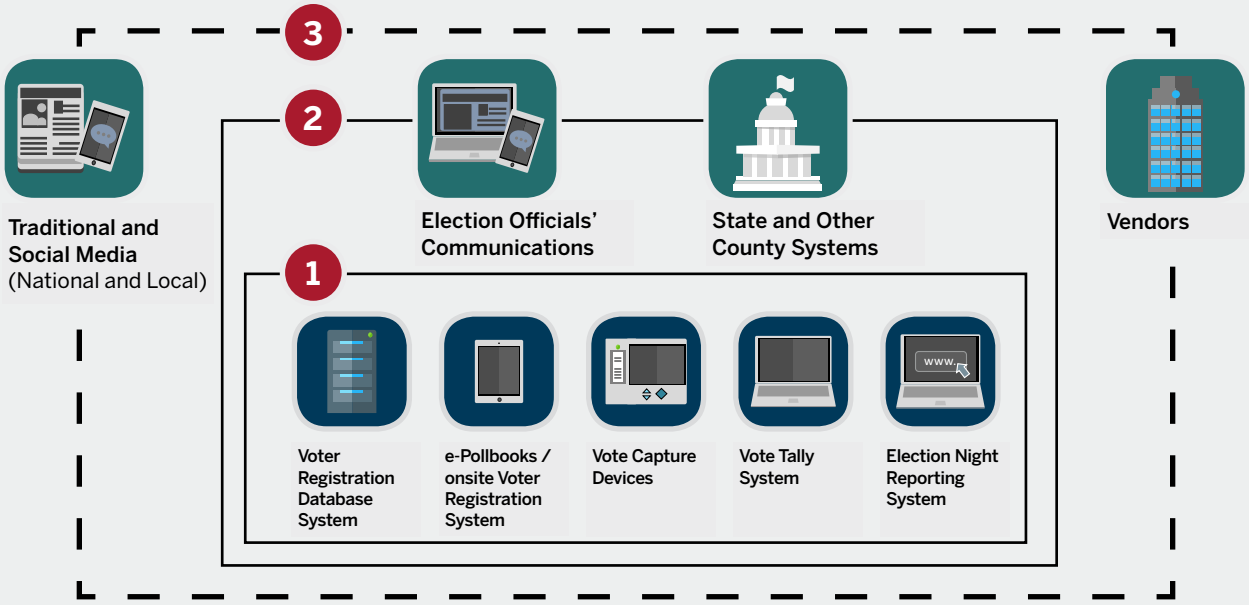
North Korea: While there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

The "How" Behind Cyber Attacks and Information Operations Targeting Elections

From a cyber perspective, every part of the election process that involves some type of electronic device or software is vulnerable to exploitation or disruption. When discussing election cyber-security, the focus is often on voting machines. However, voting machines are only one part of a complex, interconnected system. Securing elections requires securing the entire process, because any element of the system could be the weak point that a malicious actor exploits.

We have broken the election system and its components into three levels of operation relating to cyber-security risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level ❶ includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level ❷ includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. The third level ❸ involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.

ELECTION SYSTEM OVERVIEW: POTENTIAL ATTACK VECTORS



Computers and software are present in every component of the election process, which means so are vulnerabilities. Depending on a malicious actor's motives, they could look to actually undermine the integrity of the vote, diminish public confidence in the process, or both. The potential attack vectors into an election system are both technical and human. They include those who develop and maintain the system, as well as the system itself. Ultimately, most cybersecurity breaches result from malicious actors exploiting human behavior, not technical shortcomings. This is true across all sectors and industries, and election systems will likely be no exception. Vendors of election systems or election software are also easy, valuable targets for malicious actors.

THE EXTENT OF VENDOR INVOLVEMENT IN ELECTIONS

Vendors play a critical role in supporting elections at both the state and local levels: from the computers used to access information, the servers that house information, the management of the databases that contain the information, the machines used to cast and tally votes, the websites and software used to display information and results, to the software that creates ballot designs or helps transfer information across systems. Some vendors are involved on such a broad scale that they can become a single point of failure at a national or state level. For example, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. In the 2012 presidential election, this vendor produced over 100 million ballots in more than 4,500 election jurisdictions and 40 states. The same single point of failure can exist at the state level. For example, one state contracted with a single vendor to do all of its state maintenance and ballot definition files for the 2018 elections.

The following figure describes common cyber and information operations that target each level of the election system. It provides a basic overview of the threats that election officials face from malicious actors.

Cyber and Information Operations

Some of the most common means and methods behind cyber and information operations used by malicious actors to target elections.

CYBER OPERATIONS

Social engineering is a category of attack in which malicious actors manipulate their target into performing a given action or divulging certain information (often a login or password).

Spear-phishing is a social engineering attack in which malicious actors send an email attachment or link that is designed to infect a device or obtain sensitive information. Malicious actors often review a target's social media accounts and work environment to tailor an email to appear enticing and convincing.

Hacking refers to attacks that exploit or manipulate a target system in order to disrupt or gain unauthorized access.

SQL injection is a way for attackers to read and/or alter the contents of a user's database by manipulating forms that are publicly available or exposed. Properly validating any incoming information from users can help prevent this method of attack.

Port scans are similar to checking whether doors are locked and walking through those that are open. Attackers often use it to profile potential targets and conduct surveillance on the systems they are running. A skilled attacker can use this method to gain access to unprotected servers or networks.

Man in the middle (MITM) attacks occur when attackers insert themselves between two or more parties and gain access to any information in transit between those parties.

Distributed Denial of service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access. Attackers disrupt service by using multiple computers and Internet connections to flood a target with excessive traffic, causing the service to crash.

Insider threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes.

INFORMATION OPERATIONS

Information Operations (IO) include propaganda, disinformation, and other tools used to manipulate public perception. Digital technologies have enabled adversaries to conduct IO at an unprecedented scale and to an unprecedented effect. In the context of elections, adversaries might use IO to undermine trust in an election result, exacerbate political divisions, or sow confusion and dissent.

Leaking stolen information: Attackers penetrate networks to obtain and leak sensitive information. Leaking information about budgets, election system vulnerabilities, or sensitive processes can reduce public trust.

Spreading false or misleading information: Attackers may hijack official accounts, or use social media or paid ads to distribute false information (e.g., polling times/places, election results), discredit a candidate, election officials, or voting system integrity.

Amplifying divisive content: Malicious actors often use existing social or political tensions to stoke divisions, distract, and disrupt a target to divert their resources.

Interrupting service to public-facing online resources: Attackers may use this tactic to accomplish a broader strategic objective. A DoS attack can serve to undermine trust in electoral systems or government services.

Common Ground

10 Best Practices that Apply to all Election Jurisdictions

Despite variations in election systems across states and localities, our 10 best practices can make any jurisdiction more secure. The list below provides overarching, high-level concepts. In the Technical Recommendations section, we operationalize these best practices into risk-mitigating recommendations addressing five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications.

1. **Create a proactive security culture**. Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared.

   Lead by example. Senior leadership, especially Secretaries of State, Election Administrators, and other heads of municipal jurisdictions, need to set an example for the rest of the organization. Issue guidance about the necessity of applying cybersecurity standards (such as those recommended in this Playbook), stressing the importance of cybersecurity for staff by personally introducing orientations and trainings, and following up with operations personnel on a regular basis about the implementation of improved cybersecurity protections. Leaders also need to ensure that those charged with implementing a cybersecurity program have the authority to enforce policies and procedures. Without enforcement, these are only words on paper.

   Develop a detailed cyber incident response plan. As with contingency plans for physical threats, teams should understand critical election system vulnerability points and create a detailed response plan (both internal processes and communications) for any system compromise. Leadership should also mandate frequent testing of critical systems to ensure both their resilience and officials' comfort with crisis management. Officials should extensively document any real or simulated incidents and review these periodically for training purposes.

   Use external resources to assist in improving cyber defense capabilities and building expertise. Department of Homeland Security and private sector technology companies are

available to provide support for prevention and detection. Recognizing Constitutional and other legal restraints, National Guard cyber units, operating under state authorities, can also be a resource to help identify network vulnerabilities. These units are often made up of highly trained professionals involved in private sector cybersecurity.

Be diligent in selecting who is involved in election administration. Election systems qualify as national critical infrastructure, which raises the security expectations for those involved. Conduct background checks on all personnel involved in accessing sensitive information and privileged systems. Require vendors to do the same.

2. **Treat elections as an interconnected system**. Adversaries can target not only individual parts of the elections process but also the connections between them. Attackers look for seams: they seek the weakest point and move from there to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet—hacks can be executed using thumb drives and other external storage devices.

Safeguard computers and digital devices that touch the process, regardless of whether they are owned by a vendor, the state or local government, or are the personal device of an official or volunteer.

Centralize and streamline device security management by incorporating election offices into existing technology security plans.

3. **Have a paper vote record.** To protect against cyber attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data; every aspect from the ballot displayed to the voter to the recording and reporting of votes, is under control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or even to detect that an attack has occurred) after the fact.

Create an auditable paper record for every vote cast that is verified by the voter to ensure if the electronic vote count is maliciously altered, a true record still exists on paper. Make sure that this verifiable paper record has a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.*

   Embed auditing at points in the process where data integrity and accuracy are critical; for example, with voter registration records.

   Make post-election audits standard practice, using paper records to confirm electronic results.

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system.

   Require strong passwords not only for official accounts but also for key officials' private email and social media accounts. For your passwords, create `SomethingReallyLongLikeThisString`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of `$ymB01$`.

6. **Control and actively manage access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them.

   Limit the number of people with access to the system to those who need it to complete their jobs (the "who").

   Restrict what each user is authorized to do using the principle of "least privilege," meaning give users the minimum level of access that they require to perform their jobs (the "what"). For example, not every official from County A needs the ability to view or modify voter registration records in County B.

   Quickly remove those who no longer need access, regardless of their privilege level. Make this a part of standard offboarding procedures for staff.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems the most. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs.

   Configure devices with sensitive data to only be used for their specific purpose in the elections process (e.g., the software on a vote tallying computer is only what is necessary to run the election management system; or it operates on an isolated network so all wifi/bluetooth is disabled).

   Restrict the use of removable media devices (e.g., USB/thumb drives, compact discs) with these systems. A "one way, one use" policy is best.

8. **Monitor, log, and back up data.** Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross-county patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs.

   Log any changes to the voter registration database, and monitor the database with both a human check and anomaly detection software.

   The adage is that "your data is only as good as your last backup." This means that (1) backups should be regularly performed, either through automation or as part of a scheduled manual process, (2) backups should be read-only once created to prevent data corruption, and (3) backups should be regularly tested by performing a complete restore from backed-up data. Database technology vendors provide guidance and best practices specific to their technology and database architecture for validating and testing restoration of backups; consult these recommendations when developing your plan. In addition to those recommendations, ensure backups are stored in a different physical location than the master database and are physically secured.

9. **Require vendors to make security a priority.** In many states, vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. In our nationwide security survey, 97% of states and territories used a vendor in some capacity. Some vendors service multiple states— meaning an attack on one vendor could affect

many elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. (*For more details, see* **Appendix 1: Vendor Management**)

Include explicit security stipulations in requests for proposals, acquisition, and maintenance contracts to ensure that vendors follow appropriate security standards, and guarantee state and local governments' ability to test systems and software.

Remember that skepticism is healthy. Verify security claims of vendors with independent analysis or reports from trained professionals.

Require vendors to provide notification of any system breach immediately after they become aware of it.

10. Build public trust and prepare for information operations.

Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. For additional information on communication strategies and planning see the D3P "Election Cyber Incident Communications Coordination Guide" and "Election Incident Communications Plan Template".

Communicate repeatedly with the public to reinforce the message that integrity is a top priority.

Before elections are held, start informing the public about cybersecurity threats, the steps taken to counter them (withhold specific details that could aid an attacker), and your readiness to respond in the event of an attack.

Establish processes and communications materials to respond confidently and competently in the event of an attack.

Build relationships with reporters, influencers, and key stakeholders to establish trust and have good communications channels before an incident occurs. It is especially important to do this with candidates and party officials.

Routinely monitor social media, email accounts, and official websites, and establish points of contact with social media firms (e.g., Facebook, Twitter) to enable quick recovery of hacked accounts.

Security Insights by Election System

During our field research we learned a lot of great insights from election officials who are making cybersecurity a reality. This list reflects many of those ground-level insights, classified by the key components of the election system. For detailed technical specifications, refer to the Technical Recommendations section.

VRDB

- Patch and update all computers and servers that connect to the database.
- Ensure the database server is not accessible over the public Internet. Restrict which external systems can write directly to the database.
- Establish a baseline for normal data activity (new entries and edits to existing entries). Monitor activity against this baseline and investigate anomalies. Add human review for data changes—at a minimum, review weekly change summaries; ideally have an official review automated updates.
- 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.
- Require two-factor authentication for anyone to log into the database—no exceptions.
- Make frequent backups of the VRDB. Conduct routine recovery drills to ensure they work.

For Online Voter Registration

- Do NOT allow web servers to connect directly to the VRDB.
- Have mechanisms in place to mitigate DDoS attacks on the voter registration website.

For e-Pollbooks

- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Make them single-purpose devices; software on them should only be what is necessary.
- Understand how voter information is loaded onto the e-Pollbooks; cryptographically confirm the e-Pollbook file on the device matches the original file.
- Physically disable or otherwise seal exposed ports if possible.

Vote Casting Devices

- Every machine should have an individual voter-verified paper trail.
- Do election audits. Make them a regular part of the elections process.
- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Do not connect machines to any network for longer than necessary (i.e., if wifi is used to update, ensure it is enabled only for the required time window).

If vote tallies are transmitted directly from the machine, ensure the data transmission is encrypted.

Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy:" only use physical media once, from one system to a second system, then securely dispose of it.

Ballot definition files could be corrupted—secure the creation, transfer, and upload process.

Vote Tallying Systems

Vote tallying systems should be single-purpose systems, with only software installed required for running the vote tallying system—nothing else, and isolated with no network or Internet connectivity.

Electronic vote tabulation data should be encrypted when transmitted between sites.

Address security vulnerabilities by patching and updating vote tallying system devices.

Use two different forms of communication to report and confirm vote tally reports (e.g., electronic file submission, then phone call).

Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy." Only use physical media once, from one system to a second system, then securely dispose of it.

Election Night Reporting

Ensure websites are up to date and create a plan for DDoS mitigation.

Limit access/edit privileges for users, similar to VRDB access.

Prepare a contingency communications plan for disseminating results.

Verify that results shown to the public on the official ENR website match reported results.

Monitor the ENR system for anomalies in traffic or access during election night.

Conduct searches/media reviews during election night to check for false sites and social media accounts.

Internal and public-facing communications

Email: Use two-factor authentication for email accounts.

Public-facing websites beyond ENR (e.g., to communicate election day logistics): Keep sites up to date to decrease potential for manipulation; have an action plan for potential DoS; know how to recover hijacked accounts.

Official social media accounts: Use two-factor authentication. Limit access. Understand third-party apps can be a vulnerability if they are compromised. Identify points of contact and establish relationships with key social media firms for responding to issues when they arise. Know how to recover hijacked accounts.

Private social media accounts: Private accounts of key officials need to be secured as they are also likely targets.

Vendors

Require vendor security measures. Vendors can connect to every part of this system. Their internal security matters—vendor access points could be the weak link that gets exploited and corrupts other parts of the process.

Ensure security requirements and considerations are included in vendor contracting and enforced.

Technical Recommendations

Securing State Election Systems

There is no such thing as perfect security; however, there are preventative measures that make the process much more secure. In the Common Ground section, we provided best practices that apply across all election jurisdictions and some system-specific insights. In this section, we elaborate on these concepts with specific technical recommendations as they relate to five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications. As we highlighted in Common Ground, system defense is a critical first step in securing the elections process. For this reason, the majority of our recommendations fall into the category of "Protect." Because election systems are decentralized and varied in nature, not all recommendations apply to every state or locality.

As we said in the introduction, our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals. But we do want to emphasize IT professionals are critical to establishing and maintaining a secure election system and their expertise will be needed for many of our recommendations. Threats are constantly evolving and IT professionals will help you get beyond what this Playbook provides and keep you abreast of the latest threats and defenses.

Voter Registration Databases and e-Pollbooks

Voter registration databases (VRDBs) store information on registered voters in a given state. The Help America Vote Act requires that all states implement a "single, uniform, official, centralized, interactive, computerized voter registration list," unless the state has no voter registration requirement. Throughout this document, we refer to this centralized, computerized list as the VRDB.

Different states follow different processes for managing and updating their VRDB—in some states, all new entries, deletions, and edits are implemented as processes at the state level, whereas in other states this happens at the county level (with changes pushed up to the state-held "master"). In many states, ***third-party systems***, such as Health and Human Services and the Department of Motor Vehicles, provide data to the VRDB in an effort to keep voter records up to date. Some states offer ***online registration***, allowing voters to register and edit their record via a public-facing online portal connected to the VRDB. Some states offer ***same-day registration***, while others require voters to register before election day.

Closely linked to VRDBs are the pollbooks used on election day. States may choose to only use paper pollbooks, or may use ***electronic pollbooks (e-Pollbooks)*** to process voters on election day. e-Pollbooks are electronic versions of voter rolls used by polling site officials to verify legal voter registration and related details on election day. These are usually tablets or laptops and can be networked into a central voter registration system (allowing them to check and update voter records in real time, for example to allow for same-day voter registration), or they can be standalone at the precinct (containing a separate, offline copy of the electors list). Regardless of whether a state/county uses paper or e-Pollbooks, their creation requires an export of files from the VRDB for either printing or translation into an e-Pollbook compatible file.

Across both VRDBs and e-Pollbooks, states may choose to develop and maintain the software in-house, or may outsource this work to an external ***vendor***.

Core VRDB issues

KEY THREATS:

Unauthorized access to the VRDB from Internet exposure: Leaving the VRDB exposed to the Internet makes it vulnerable to attacks. Once it is connected to the database, an attacker can add, edit, or delete voters, allowing for false votes to be cast on election day or forcing voters to cast provisional ballots. Even if this does not affect actual vote outcomes, the perception of vote manipulation or voter suppression can significantly undermine the credibility of an election.

Maintenance: An insufficient or poorly timed maintenance and patching regime leaves security vulnerabilities open and can expose the VRDB to attacks.

Account compromise: Attackers might compromise the accounts of election officials with access to the VRDB; without proper controls in place this could allow the attacker to add, edit, or delete voter entries. In the absence of proper logging and monitoring, these changes may go unnoticed until election day and affect the ability of voters to cast ballots.

Third-party system compromise: Third-party systems (e.g., DMV, HHS) linking into the VRDB can be compromised, or the transmission of these entries to the database could be compromised along the way. If these systems are allowed to feed directly into the VRDB, or if the review and approval process at the state and county level is insufficient, there is a risk that the compromise could allow malicious actors to manipulate voter status.

Recommended actions:

Identify

Map how other systems connect to the VRDB. They will commonly be connected to sync or add voter information (e.g., from DMV records).

Know where the VRDB is hosted and what defenses exist on the servers and the underlying network infrastructure.

Know what accounts have access and what level of access each account has (e.g., can a county official change records from other counties?). Use a test account to verify that restrictions are operating as intended.

Determine which of the servers can be accessed over the Internet. Close connections to any that do not require access.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can edit the VRDB. Account security is crucial for all VRDB users and especially those with elevated or administrative privileges.

Conduct penetration tests, source code audits, and encourage vulnerability discovery efforts. Regardless of whether your VRDB software is built in-house or by vendors, third-party auditing and penetration testing should be performed to provide awareness of security vulnerabilities. Develop and maintain a continuous program that tests your organization's susceptibility to spear phishing and other social engineering attempts. It is important to do this regularly, both to spot new vulnerabilities that might arise, and to prevent staff from becoming complacent.

Apply software updates and patches. Applying software updates and patches on all devices connecting to the VRDB is essential to preventing malicious actors from gaining access. Check for patch signatures to ensure they are authentic. Using endpoint management software and vulnerability software on official computers can help automate the patching process to ensure systems stay up to date.

> To prevent interference with election day operations, **establish cut-off days for applying and testing patches** to ensure optimal functionality during election periods. Only critical updates should be done after the cut-off window and all patches should be tested for functionality as well as security.
>
> **Create automated scans** to look for vulnerabilities on the VRDB portal.

Ensure that your underlying database server is not accessible over the Internet.

Restrict external systems' access to the VRDB. Data from other systems (e.g., the DMV) should go through validation (either manual or automated) rather than allowing those systems to directly write to the database. This prevents the database from being directly edited if an external system is compromised.

Log changes. As a rule, changes to the VRDB should be recorded securely and be reviewed, preferably both by a human and an automated system. Establish a baseline for normal data activity (e.g., new entries, edits to existing entries, change in voter status) so that atypical behavior can trigger an alert.

Limit account access to the VRDB. Restrict access to the database to those who need it and diligently maintain and review this access list. For example, state or local offices responsible for updating voter registration information require access. However, the software developers who designed the system do not. Account management includes revoking the access of old employee accounts immediately after they depart or change roles. Vendors responsible for the software will need access, but should not retain that access any longer than necessary.

Implementing these limitations requires an individual to be responsible for constantly managing accounts, ensuring existing accounts belong only to those who need them, and that system permission changes were approved.

Permissions Management for VRDB accounts. Everyone who has an account should be given specific permissions that dictate what they can and cannot do. More people with more access means an increase in potential avenues of attack on the VRDB, so limit the degree of access for each account to only what is necessary for that employee to do their job.

The most common levels of permission variation are "read," "write," and "admin" access. Someone with "read" access can only read the data, but not alter it; someone with "write" access can change data; and someone with "admin" access can alter permissions for other users.

Even within those levels of permissions the scope of access should be tailored. For example, a county administrator may need access to their own county's information, but should not be able to access information from another county.

Consider implementing permission restrictions that limit the number of changes one user can make during a certain time window to stay in line with normal activity patterns—this helps guard against both insider threats and account compromise.

Require users to access the VRDB portal using a VPN. This ensures that even if an account is compromised, the attacker is unable to use it without VPN credentials.

Whitelisting can also be used to limit either what devices a user can connect from or which locations. Paired with a device inventory database, requiring device certificates will allow you to restrict access to managed devices that are verified as secure. Another option is IP whitelisting, which can restrict access to users at specific location. This would require coordination with remote offices' IT departments to identify what addresses should be whitelisted. Using IP whitelists would force an attacker to compromise a machine at one of the locations before they were able to begin an attack against the VRDB.

Establish policy that does not allow connections to the VRDB from public, unauthorized, or unknown devices.

Detect

Monitor activity against a baseline and investigate anomalies. This allows you to notice unusual trends that deviate from the norm. At a minimum, this should be a technical (automated) check which occurs at both the state and county level. Automated monitoring of anomalies at the state level is critical to detect broad changes across the state that may not be noticeable when monitoring only at the individual county level.

Incorporate a human review into data change monitoring to augment technical monitoring. Experienced election officials providing human monitoring at the local level may reveal subtle manipulations. Election officials should trust their instincts—they are more

familiar with this data than anyone else. Empower these officials to flag suspicious behavior or anomalies and investigate them. While human review of every record change is not realistic for all localities, weekly change summaries should be required at a minimum.

Monitor permission changes: Make sure that when changes are made, they are reviewable by those with similar access levels. Create the framework for conducting regular reviews of those changes. This process will allow unusual activity to be detected sooner.

Mail confirmation of changes in registration to voters (ideally both to their old and new address).

Respond

If the incident involved an attacker gaining access to VRDB, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If a physical machine was compromised, disconnect the machine from the network and seek professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Execute the recovery plan during an incident or after one occurs. Include the following categories in your plan: Recovery planning, improvements, and communications.

Public communications around a voter registration-related incident is a CRITICALLY IMPORTANT issue when it comes to public trust and elections transparency. It must be deliberately executed with tremendous care. See D3P's *Elections Cyber Incident Communications Plan Template*.

Practice restoring from VRDB backups. If there is a second live VRDB system, be sure to practice using the secondary system.

Lessons learned should be shared and incorporated into the existing recovery plan. Where possible, update your system to prevent a similar failure or exploit from occuring again in the future.

Vendor Considerations

The most common forms of vendor support for voter registration databases are:

- Vendors building and maintaining the VRDB
- Vendor building and state or county maintaining of the VRDB (to include modifications to initial vendor build)
- Vendor and state jointly building and maintaining
- Third party vendor used to assist with maintenance

The General Vendor Recommendations 1-8 at the bottom of the Technical Recommendations section provide best practices for working with vendors and mitigating potential cyber vulnerabilities. The type of vendor involvement and timeframe (set time period involvement versus continuous) will impact how they apply for each state/county. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Online Voter Registration

States that offer online registration are exposed to the following additional threats:

KEY THREATS:

Website spoofing: Attackers could pose as the official website to either give voters the illusion that their information is updated or in an attempt to capture that information.

Distributed Denial of Service: Attackers can conduct DDoS attacks on the public-facing voter registration website, preventing voters from registering and potentially discouraging them from participation.

External connectivity: An unsecured website presents another vector for a malicious actor to penetrate the VRDB. If it is not properly secured, an attacker may be able to use it to change any vote record.

Large-scale data alteration: An attacker could use information leaked on the Internet to impersonate many different voters and attempt to update their registration details.

Recommended actions:

Identify

- Know who the domain name registrar and web hosting provider are and how to contact them.
- Determine who is responsible for keeping the website software up-to-date.
- Know who has the ability to edit the website.

Protect

- Do NOT allow web servers to connect directly to the VRDB. This restriction significantly reduces the possibility of a website vulnerability leading to a compromise of voter records.
- Require a CAPTCHA to change a voter's registration. This is a short task, ranging from clicking a checkbox to typing the characters shown in an image, which verifies that an online form is being submitted by a human and not a machine. It increases the difficulty of a computer program changing hundreds or thousands of voter registrations at once.
- Protect the online voter registration website against DDoS attacks.
- See the **Website** section for additional details on securing the public-facing component.

e-Pollbooks

KEY THREATS:

e-Pollbook Data Manipulation: A malicious actor is able to gain access to the device either using a wireless connection or because the physical device was not properly secured. Once on the device they are able to manipulate the voting roll—either deleting or altering existing voter registration data.

Altering of State Voter Roll via e-Pollbook: If an e-Pollbook has a live connection to the state election day voter roll, compromising one device could be used to change statewide records.

Maintenance/patching of e-Pollbooks: The difficulty in which an e-Pollbook device is compromised depends heavily on whether it is updated and patched. Failure to do so will provide malicious actors an opening into the device.

Recommended actions:

Identify

Examine all the possible functionalities of the device and identify the components you intend to use. Specifically pay attention to the wireless and networking functionality.

Know what kind of network connections your e-Pollbooks need.

Understand how voter information is loaded onto the e-Pollbooks.

Protect

E-Pollbooks should be single-purpose devices. Software on the device should be limited to what is necessary for their use.

Verify the integrity of the e-Pollbook file.

Cross-check the data on the pollbook with what is in the VRDB.

Use digital signatures and hashes to verify the integrity of data contained in voter roll files that are transferred between systems and to ensure data has not been maliciously altered or compromised. If using a method that requires data transmission over a cellular network or the public Internet, use a virtual private network (VPN) to secure those transmissions.

VERIFYING FILE INTEGRITY USING HASHES AND DIGITAL SIGNATURES

A hash is like a fingerprint for digital files—the *hash* of a file will not change unless the actual file changes. Using a hash while transferring files will allow you to confirm that the file has not been altered in transit if the hashes computed by each party are the same. If you decide to use a hash, transfer it through a different channel than you used to obtain the files and compare it to the hash you compute. By sending them separately, such as downloading the file from a website and reading out the hash over the phone, you prevent the attacker from changing the hash at the same time as the file.

A more secure option is to use a digital signature. It is a form of encryption which is equivalent to a seal on a physical document; it guarantees that the file came from a specific trusted source and that its contents have not been modified in transit.

Ensure all devices are updated and patched. Test the e-Pollbook to ensure that it is fully functional after patches have been applied.

If you do not need the e-Pollbook to be connected to a vendor, VRDB, or the Internet while voting is taking place: **turn off bluetooth and wireless capabilities on the devices.** It is better to disable these functions at the hardware level (e.g., removing the wireless card) than to change a setting whenever possible.

If you need to connect to external systems:

- **Connect over a VPN** or other encrypted channel.
- **Ensure that the entire setup is preconfigured** and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
- **Do not connect e-Pollbooks directly to the VRDB.** Set up a separate system (essentially a copy of the VRDB) to handle changes to voter information, which prevents the VRDB from being impacted if an e-Pollbook is compromised.
- **Restrict edit access only to juridictions that need it.** If state law requires you to vote in precinct and there is not same-day registration, an e-Pollbook in one precinct should not be able to modify the voter's record from another precinct.

Have a paper backup of the e-Pollbook.

Ensure physical security. Cover exposed ports (e.g., USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. Do not use anything other than the charging cords provided with the e-Pollbook on receipt (e.g., do not use an iPhone charger or other similar charger that is not actually part of the e-Pollbook election day pack).

Detect

Monitor data changes. Counties or vendors, as applicable, should monitor voter roll files for anomalies in changes or access. Implement data controls around normal data activity that prevent large-scale changes.

Perform vulnerability scans of e-Pollbook devices to identify those that do not have the latest security updates. Apply patches to minimize vulnerabilities.

Respond

If the incident involved an attacker gaining access to a networked voter roll file shared beyond a single polling site, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If the e-Pollbook device was compromised, disconnect the machine from the network and seek out professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Have a backup paper copy of the pollbook on site and backup devices pre-programmed for deployment to sites, if necessary.

Vendor Considerations

The most common forms of vendor support for e-Pollbooks are:

- Building and/or maintaining of e-Pollbook devices and software.
  - Can overlap with vendor support for VRDBs.
  - Can involve live monitoring of e-Pollbook operations on election day.
- Building electronic voter roll files for e-Pollbooks based on VRDB info where a compromise of the vendor could result in voters being missing, or incorrectly added to, the roll.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Vote Casting Devices

Overview: Vote casting devices serve as the primary conduit for the actual ballot marking or mark recording process on election day. Most states and counties today use some variation on two types of vote casting devices:

> **Optical Scanner (OS) or Digital Image Scanner:** A machine that scans (and often digitally records an image of) marked paper ballots. Voters cast a ballot via traditional pen and paper, an electronic ballot marking device, or some alternative marking method. The marked paper ballots are then run through these scanning machines which records the appropriately marked vote for each race, and then calculates running vote totals for all ballots scanned on the machine. The machine prints a total result after polls close. The initial paper ballot ensures that a physical record exists for audit or other vote verification purposes.

> **Direct Recording Electronic (DRE):** A DRE system presents a digital ballot image to a voter, collects the voter's selections, and records those choices directly onto electronic media. DREs may be fitted with voter-verified paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction.

In recent years, alternate voting methods, particularly vote-by-mail and early voting, are becoming increasingly popular with voters. These jurisdictions often utilize central count facilities where paper ballots are consolidated for tallying. At central count facilities larger variations of the optical scanner/digital image scanner are often used for paper ballot counting.

KEY THREATS:

Device tampering: Voting machines can be compromised via physical tampering (including using removable media) or through external connectivity (e.g., WiFi). This would allow the attacker to change the reported vote information.

Inability to detect tampering: Some DRE machines do not produce a VVPAT (because optical scanner systems scan paper ballots, they do not face this threat). Should a malicious actor compromise such a machine, votes could be lost and results thrown into question.

Recommended actions:

Identify

Examine all the possible functionalities of the device and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.

Know the certification status of all your equipment. The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

Protect

If you have a DRE machine that does not produce a paper trail, **you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**

Physical Security/Access Seals. Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.

Penetration test systems. Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote casting devices.

Restrict device functionality to what is required. Even if you have disabled a feature through a settings page (such as wifi connectivity), those features could still be exploited. You should not trust that toggling a switch in software will actually disable the functionality. If possible, the hardware should be removed.

Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem. If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.

> **Create a copy of the results** (either a printout or by saving it to removable media) before you connect to the network.

If removable media is used to transfer data (e.g., ballot definition files, vote tallies):

> **Have a procurement strategy for devices.** Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.

> **Protect device chain of custody.** Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical

record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.

One-way/one-time use: Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.

Scan media devices for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

Detect

Perform logic and accuracy testing of the programmed device.

Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

Respond and Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Handling ballot definition files and other software updates

KEY THREATS

Supply chain interdiction: A malicious actor could use vendors as a pathway to plant malware to modify or compromise a ballot definition file before it reaches the hands of election officials.

Manipulation of ballot definition files: If an attacker obtains access to the original ballot definition file, this could leave machines susceptible to destructive attacks and/or could affect tallies.

Recommended actions:

Identify

Determine who is responsible for, and what machines are being used, to create the ballot definition file.

Determine how the ballot definition file is being transmitted to the vote casting device.

Protect

Treat the ballot definition file as critical information. As such, limit its exposure to compromise as much as possible. The system used to develop the file should be isolated from external network connectivity. Place a tamper-evident seal over the media containing the ballot definition file.

Conduct testing (e.g., logic and accuracy, parallel testing) on the systems that the ballot definition files have been loaded onto before deploying them for use.

Review ballot definition file source code to prevent malicious code distribution. When possible, review source code before final distribution of ballot definition files to avoid dissemination of malicious code.

Secure the creation mechanism of the ballot definition file: The ballot files should be generated on a secure single-purpose and air-gapped machine

Secure the transmission of the file:

If possible, use digital signatures on the file. Forcing the voting machines to verify the file signature before loading it will prevent attempts to change the ballot files after it has been created.

If using removable devices to transfer the files, follow all best practices, including one-way and one-time use. The section on vote casting devices above discusses more specific recommendations for removable media.

Detect

Verify the seals over media containing the ballot definition file.

Scan ballot definition files for malware. If you detect abnormalities, don't use the files and contact forensic experts for assistance.

Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors often interact with ballot files by:

- Creating the files themselves
- Transferring the ballot files to the voting machines

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Vote Tallying System

Vote tallying covers the various devices and networks used to tabulate ballots and aggregate results. Based on differences in setup across states and counties, this process can start at the polling site (for example, precinct count optical scanners that tabulate ballots onsite), or at more centralized counting facilities. In many instances vote tallying is conducted at the county level, where voting sites through a variety of methods (e.g., phone call, email, thumb drive/USB) provide counties with their respective vote tally totals. This section discusses common threats and remedies seen across many system set-ups.

KEY THREATS:

Manipulation of tabulation systems: A compromised tallying machine at a polling site or central counting facility could allow an attacker to directly manipulate tallies before they are transmitted to the county or state.

Data transmission with removable media: USB devices—and other portable physical media—are often used to transmit results from precincts or centralized counting facilities to segmented county/state networks. USB devices can be exposed to malware and compromised at the supplier level or through a previous use in an infected machine. This compromise could result in manipulated data and could also lead the tallying machine itself to become compromised, exposing the system to future exploits.

Networked data transmission: In tallying setups where votes are tabulated at the polling station and transmitted to the county, or are transmitted from the county to the state through a system other than the election night reporting system, configuration errors in the modem, wifi, or cellular network connections used for transmission can leave the process vulnerable to "man-in-the-middle" attacks. These allow adversaries to manipulate results before they are received at the county (or state) level.

Denial of service: Counties or, where relevant, states, receive results from precinct or centralized counting facilities over the network. Servers can be targeted with a DoS attack by an adversary, resulting in delays in vote reporting during election night.

Recommended actions:

Identify

Know the certification status of all your equipment. The EAC's Voluntary Voting System Guidelines (VVSG) provide federal level certification standards. Many states have their own certification process.

Protect

Vote tallying systems should be isolated from any networks or overall Internet connectivity (commonly referred to as "air-gapped"). This includes connecting to voting machine modems. In the case where you cannot achieve total isolation, restrict network access to precincts and counties to prevent outsiders from accessing or slowing down the system. Again, the best practice is to keep these machines totally isolated and to transfer results to them using removable media as they arrive. As for all removable media, practice the "one-way, one-use" rule.

Use a dedicated single-use system for vote tallying. Using a system solely for vote tallying and disabling unnecessary functionality, like network connection, can limit exposure to attackers.

Require strong passwords and implement two-factor authentication to access the vote tally system device. There are two-factor authentication methods that do not require network connectivity, and that can be implemented.

Use a digital signature to verify the source of vote tallies. Requiring each voting machine to digitally sign its report will prevent a malicious actor from introducing fake results into the tally process.

Keep devices up to date and fully patched. Despite the tally system being air-gapped, it is still important to keep the software on them updated. Review available updates, test how they work with your system, and apply them. You should establish a cut-off date prior to the election after which you will not change the software in order to provide enough time to test the system.

System testing. Include the tallying system in your tests of the system. While conducting penetration tests, teams should look for ways they could access these machines despite the air gap (including testing the physical security) and other ways to force errors in the tallying process.

Detect

Report vote tally totals using multiple forms of communication (redundant communication). For example, electronic vote tally submissions should be confirmed with a follow-up call or text.

Recover

If the electronic system is compromised, implement hand-count procedures.

Vendor Considerations

In many cases, the machines used to tally results will have been provided by vendors who will be involved in the maintenance of those machines. A compromise at this level could cause vote totals to be calculated incorrectly, compromising public trust in the election even if the correct totals are eventually reported.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Election Night Reporting (ENR)

Election night reporting (ENR) consists of the systems and processes for aggregating and communicating the unofficial election results to the public and media after polls close, usually via a website. Counties and states may also report election night results via social media—please see the Internal and Public-facing Communications section for best practice in securing social media accounts. ENR setups vary by state across three principal dimensions defined below:

How ENR relates to the vote tallying process. ENR can be closely linked to the vote tallying process (e.g., a state's non-public vote tallying system might automatically submit results to the state's public ENR website), or can be run separately and in addition to the tallying process.

Whether ENR is run by the state, counties, or a combination of both. Most states run ENR centrally, with counties (or in some cases municipalities) submitting results to the state via a centralized ENR system. In some of these cases, the counties run separate, additional ENR systems (e.g., to provide further granularity on results). In a small number of states, ENR is managed at the county (or municipality) level.

Who builds/maintains the ENR system. Regardless of whether ENR is run at the state or county level, ENR systems can be developed and managed in-house (by the state or county), developed by a vendor but managed in-house, or developed and run by a vendor.

KEY THREATS:

Transmission: In a state-run ENR setup, counties submit their vote reports to the centralized system provided by the state. A configuration error could make this transmission vulnerable to "man-in-the-middle" attacks, where adversaries manipulate vote reports before they are received by the state.

Manipulation of ENR systems: Configuration errors can leave ENR systems vulnerable to exploits or unauthorized access, allowing adversaries to manipulate the vote counts after they have been received in the (state or county) ENR system.

Denial of service: In a state-run ENR set-up, a DoS attack on the transmission of ENR results can lead to a lack of results being reported for one or more counties. In addition, attackers can conduct DoS attacks on the public-facing ENR website, making result reporting unavailable to the public/media altogether during election night.

KEY THREATS (CONTINUED)

Website spoofing: Attackers could redirect public inquiries to a spoofed website, which pretends to be the official ENR system but in reality is controlled by a malicious actor. For example, this could be used in disinformation campaigns to depress voter turnout by saying an election has already been called.

Recommended actions:

Our recommendations should be implemented by the county, state, or external vendor, as appropriate.

Identify

Identify which offices need access to the ENR site or other medium through which they report and consolidate results.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can access the ENR system.

Secure transmission channels. Require users to authenticate themselves when adding result information and restrict the results they are able to change to only what is within their purview. Ensure all network traffic is secure (e.g., enable SSL on a web-based portal).

Limit access through restricting write privileges for users across the state and counties or within the county as applicable. In state-led ENR systems, specifically ensure that each county can only edit its own vote reports (not those of other counties).

Log incoming election results to help trace and correct inaccurate reports.

Prepare a contingency communications plan for disseminating results if the primary medium is unavailable.

Publicly communicate about ENR process to preempt spoofing. Communicate clearly, ahead of any election, how the state or county will report vote results during election night, to preempt false ENR websites from popping up.

Protect ENR websites against DoS attacks. See Website section for additional recommendations.

Report election night results using multiple forms of communication. They should be confirmed over a second channel; for example, a follow-up call, on top of being sent through the primary channel.

Detect

Each county/precinct should verify that results shown to the public on the official ENR website match the results they reported.

Monitor the ENR system for anomalies in traffic or access during election night. Especially monitor any attempts to change the displayed results (e.g., failed login attempts to the portal) or traffic that may be part of a DoS attack.

Respond and Recover

Public communications around election night reporting are critical. Have a backup plan for how to publicize either that your reporting website is showing no results, or incorrect results. Include the specifics in your communications incident response plan.

Vendor Considerations

Vendors are often responsible for building and/or running both the system for updating results and the webpage that displays those results to the public.

> Be sure that you have an internal (state and local level) backup plan for how to publish results if the vendor system is unavailable.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Internal and Public-facing Communications

Running successful elections requires extensive communication—both within state/county election teams, and with the public. This tends to consist of four key communication channels: internal email communication, official election-related websites, official social media accounts, and the private social media accounts of key officials. All of these communication channels could come under attack by adversaries who abuse them to cause confusion about election logistics before or during election day, and/or to undermine the credibility of the election overall.

INTERNAL COMMUNICATION

Email communication ahead of and during the election is crucial for the election team to coordinate activity internally among states, counties, and precincts/polling stations.

KEY THREATS:

Account compromise: Attackers could compromise key officials' email accounts to send out false information to members of the election team—for example, asking for polling stations to close early or for polling stations to switch to paper pollbooks due to an alleged issue with e-Pollbooks (resulting in delays and lines forming). In addition, compromised accounts could be used to distribute malware across the election team's devices. Clearly, access to the email account of any member of the election team—even at a low level in the organization—exponentially increases the chances of subsequent attacks on the email accounts of more senior members of the election team succeeding.

Recommended action:

Implement two-factor authentication for all official accounts. In most cases, adding a second factor will be enough to prevent an attacker from compromising an account. In addition to this, require strong passwords.

Require all messages to come from official accounts. While officials should take steps to secure their personal accounts as well, all official communication should be done through accounts that have been carefully secured by your IT department.

PUBLIC-FACING COMMUNICATION

Election officials communicate extensively with the public through both ***official election websites*** and ***official social media accounts*** (e.g., Election Board's Twitter account, Secretary of State's official Facebook account). This communication is separate from, and in addition to, election night reporting (which we cover in the section above), and includes, for example, communication to raise awareness of upcoming elections, key deadlines, (e.g., for online registration) and election day logistics (e.g., poll locations, opening hours, ID requirements).

While not officially part of a state's or county's public-facing communication, the ***private social media accounts of key officials*** (e.g., the Secretary of State's private Facebook account) could be used to communicate false election-related information to the public. These should be protected with the same care as the organization's public accounts.

Official Websites

KEY THREATS

Website manipulation (e.g., changing information on polling place location): Malicious actors could look to sow confusion or discourage voters by manipulating the information on official websites. For example, attackers could alter polling site locations and times to make it harder for voters to find their designated vote site

Spoofed websites: To sow distrust in the process, attackers may replicate the official state or county website and post the opposite results than is being reported—for instance the winner of Race A is now the loser.

Distributed denial of service attacks: Similar to voter registration sites, attackers could attempt to shut down official websites on election day to inhibit voters from knowing their designated voting location.

Recommended actions:

Identify

Know who your web hosting provider is and how to contact them.

Determine who is responsible for keeping website software up-to-date.

Know who has the ability to edit your website.

Protect

Have automated procedures to keep software (e.g., Wordpress, Apache) up-to-date. Website software needs to be updated on a regular basis in order to patch vulnerabilities as they are discovered. Have a system for tracking what version of software you are using and what vulnerabilities are discovered and ensure that those vulnerabilities are patched.

Conduct penetration testing and security audits for all resources. Regardless of whether your website was developed by your staff or by vendors, a third-party audit and penetration test can identify vulnerabilities. This should be done anytime a major change is made to website software.

Ensure that developers have been trained on what the common attack vectors are. One good guide for these is the Open Web Application Security Practice (OWASP) Top-10 list.

Ensure sufficient capacity to receive increased site traffic during high-use periods. Provision servers accordingly and conduct load tests ahead of time to be sure that the infrastructure can handle the additional traffic.

Ensure that your website is protected against DDoS attacks and monitor traffic to detect anomalies. Free DDoS protection and mitigation services are available, such as Google's Project Shield and Cloudflare's Athenian Project.

Detect

Have a dedicated person with the job of looking for fake content or spoofed websites in search engine results.

Recover

Have a backup version of the website hosted elsewhere in case the primary site goes down. This version should contain only barebones, essential information (e.g., precinct locations / hours).

Vendor Considerations

Official websites are often created by vendors, and in many cases vendors are also responsible for making changes to them.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Social Media (official and private accounts)

KEY THREATS:

Account compromise: Attackers use spear-phishing to learn the username and password for the county Facebook page which did not have two factor authentication enabled. The attackers then post misinformation about certain voting sites having several hour wait times and direct voters to alternate sites which are then overwhelmed.

Fake accounts: Malicious actors create a fake Twitter account for an election official (e.g., Secretary of State, Election Director) which gains traction because it is retweeted by a bot farm controlling several thousand accounts. The fake account then posts the wrong unofficial election results after polls close.

Recommended actions:

Identify

Be cognizant of which accounts could be used to disseminate information about an election. This includes accounts for your organization, as well as both the professional and personal accounts for officials. Determine who has access to each of these accounts.

Identify points of contact and establish relationships with key social media firms like Facebook and Twitter. Confirm a point of contact in case social media accounts connected to the election are compromised; or in case malicious fake accounts surface. Confirm the requirements for regaining control over accounts and shutting down malicious fake accounts.

Know key stakeholders for communication channels (media, political party contacts, advocacy groups, etc.)

Protect

Inform key officials that their private accounts might be targeted. Establish clear policies for officials and staff on use of private accounts for sharing official information, including policies for communicating indications of malicious cyber activity.

Secure social media accounts. Social media services such as Twitter and Facebook support two-factor authentication for accounts, and enabling this capability is the best step you can take to keep your accounts secure and should be done for both official accounts and the personal accounts of key personnel. In addition to this, require that the passwords for your official accounts be secure.

Understand third-party apps can be a vulnerability if they are compromised. Use third-party social media management platforms judiciously to reduce your threat surface. Periodically review linked accounts and connected apps and remove any that are no longer required.

Detect

Have a dedicated person responsible for looking for fake content in search engine results or on social media.

Recover

See the **Election Cyber Incident Communications Playbook** and **Election Cyber Incident Communications Plan Template** *for State and Local Election Officials*.

Engage with social media firms to recover/disable accounts.

If an account has been compromised, review what permissions it has granted to third-party apps and reset them to prevent further access by unauthorized parties.

Vendor Considerations

If you need to use a third-party social media application to manage social media accounts, then research the applications security practices and access policies to understand what vulnerabilities using it presents.

Vendor Considerations

*(See **Appendix 1, Vendor Selection and Management**, for best practices related to vendor contracts.)*

1. **Clearly define** the division of labor and responsibilities between the vendor and the local officials. Identify any gaps between the two parties and specifically assign responsibility to fill those gaps.
2. **Create and enforce contractual requirements.** Require vendors to adhere to well-defined security practices ensuring safe handling and protection of data.
3. **Require vendor assessments.** State/local contracts with vendors should include provisions requiring vendors to conduct third-party vulnerability assessments of their systems and share the results. See vendor appendix for more details.
4. **Mandate that vendors permit penetration testing of systems**, including voting machines, as part of RFP contracts.
5. **Secure access.** Unnecessary personnel should not have access to systems. Vendors who need access to secure systems should be granted temporary credentials and exercise that access under the supervision of a state or county official. Once a developer has finished building an application, ensure that they do not have access to the production system.
6. **Secure data transmissions.** Require vendor systems to use digital signatures to ensure the integrity of all received and transmitted files.
7. **Require audit logs for any vendor-run system.**
8. **Mandate patching** as part of a vendor request for proposal (RFP) contracts and ensure that the patching is conducted securely and frequently.

Appendices

Appendix 1. **Vendor Selection and Management**

Election system vendors are key partners in addressing cybersecurity risks. Their systems, by definition, increase the attack surface and present additional risk factors that must be mitigated to address cyber threats. Since vendors often develop and maintain systems critical to elections (such as ballot counting equipment and VRDBs), it is crucial to ensure that their protocols and practices meet rigorous cybersecurity standards.

Performing a security risk assessment of vendors during the request for proposal (RFP) process can reveal vendor vulnerabilities and reduce future exposure to external attacks. This risk assessment should be conducted in two steps: 1) during the procurement process, ensure that all vendors are willing and able to comply with security standards that meet, or exceed, election agency expectations, and 2) validate vendors' ability to meet their commitments via thorough due diligence, and ensure that vendors are reviewed periodically, not just at the time of selection.

When assessing a vendor, there are three general principles to consider:

> **Organizational security practices.** Evaluate the extent to which cybersecurity activities and outcomes are embedded across the organization, from the executive level to the implementation/operations level, such as hiring, subcontracting, policies and procedures, cybersecurity awareness and training, network and system management, vendor management, vulnerability management, and software/hardware development.

> **Ongoing partnership capacity.** Vendors should be your partners in addressing cybersecurity risks! Evaluate the levels of transparency associated with their cybersecurity processes, and to what extent they will collaborate with you on key security risk-mitigation activities, including consequence management after a cyber incident. These would include code reviews, vulnerability scans, patching, and implementing controls to strengthen their security posture, while also closing critical gaps.

> **Maintenance strategy.** Cybersecurity is not a "point in time" activity and you may have a long-term relationship with a vendor. As new attacks emerge, software and hardware should be updated commensurate with the nature of evolving risks and the state of the art in cybersecurity safeguards. This expectation must be built into vendor contracts.

Specific security requirements for vendor agreements

With the above principles in mind, security requirements should be clarified in RFPs to ensure that vendors are limiting cyber risks while working with the states or counties. The following set of core security requirements are not exhaustive, but they do provide a foundation to include in vendor RFPs. Each vendor bidder should be required to:

- State how system access in the proposed solution will be managed.
- Describe what type of data will be processed and how it will flow through the system, including any relevant data processing or data storage vendors and, if applicable, locations.
- Describe security at all layers of the solution—application, server, database, data exchange, and network security layers should all have the ability to manage access and privileges at a granular level.
- Describe how security measures will protect data for the entire data life cycle, ensuring that data remains protected for as long as it is in the control of the vendor and, when required, is securely destroyed.
- Describe how the proposed solution meets or exceeds compliance with all state- or county-level security requirements.
- Describe how encryption will be implemented for data "at-rest" and "in-transit."
- Describe how User Access Management will be handled under the principle of "least privilege" (i.e., provide only the minimum level of access required for the user to perform his or her core job), as well as how it will be maintained and pared over time.
- In your Service Level Agreements (SLAs), include clauses for vendors to notify you in the event of a cybersecurity breach of their systems or other unauthorized access immediately after they become aware and to cooperate with any consequential investigation, response, and mitigation.

Transparency requirements should also be established in the RFP to ensure that officials have the ability to perform due diligence and conduct independent security risk assessments. Moreover, transparency will aid in identifying potential conflicts of interest. Non-Disclosure Agreements will protect vendor proprietary information, in exchange for receiving access to:

- **Corporate governance relating to security practices.** Officials should have the ability to review vendors' security policies, standards, and guidelines. They should be able to

assess whether these are implemented in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

Internal security audits. State officials should perform audits (and retain the right to do so) of a vendor's security practices and protocols. This activity provides assurance that the vendor's cybersecurity practices are robust and meet state and local security standards, including those outlined in the above section. This is especially important in the months and years after vendor contracts are signed. Vendor-provided system logs should be contractually viewed as customer owned data not vendor owned data. For instance, voting system audit logs should be readily available to election officials and considered by contract as their data.

Source code. Election officials should have access to the source code for any critical system to perform internal or third-party reviews. This can be a sensitive subject because of intellectual property concerns, but being able to independently audit vendor-created code allows officials to ensure that the code is secure. It also guarantees that the code does not contain any potentially unwanted networking requests, transfers of sensitive information, or modifications to key algorithms and counting mechanisms.

Penetration testing. Penetration testing is a critical element in ensuring that vulnerabilities in vendor environments are proactively identified and closed. The RFP should clearly include requirements for the vendor to allow penetration-testing by state officials or third parties of their systems to discover weaknesses. Vendors may resist these provisions, especially if they hold broader state contracts that could be affected if vulnerabilities are discovered. Nonetheless, conducting these tests represents the best way to identify cracks in critical infrastructure before malicious actors do, and should be part of any contract with vendors who work on and maintain these systems.

Data flow transparency. Officials should have full visibility into data flows for voting system data. Therefore, it is essential for officials to request that the vendor provide its applicable data retention and destruction policies, a list of relevant physical locations where data will be processed, stored, or otherwise accessed, and an exhaustive list of subcontractors who may process, store, or otherwise access voting data or systems. Depending on the nature of the vendor's services, it may be necessary to impose flow-down security and audit requirements on subcontractors, including on the vendor's infrastructure vendors, or, if relevant, to explicitly restrict data storage locations.

Appendix 2. **Election Audits**

While following cybersecurity best practices will help deter and defend against malicious actors, there is no such thing as an impenetrable system. Even if an election system is not attacked, software or hardware errors could lead to an incorrect vote tally. To protect against technical manipulation or failures undermining the process, elections should be "software independent," meaning that they do not rely on a computer to provide a vote count, but instead have an independent auditable paper record for definitive results.

You should conduct a post-election statistical audit with these paper voting records. Such audits provide two critical benefits: (1) they offer transparency and build public confidence in the system and process; (2) they confirm the accuracy of the results, or, on rare occasion, identify that an error has occurred and must be addressed. Post-election audits are designed to be an independent confirmation of the election result. These audits should be observable and reproducible by external third parties. This requires making data necessary to conduct the audit publicly available to independent parties so that they can confirm audit results.

There are two main methods of post-election audits. Since performing a full hand-count of every ballot is extremely time-intensive and the results will likely be inaccurate, other methods are used to inspect the results with a manageable amount of work.

The first audit type uses a fixed percentage of ballots cast. This method, however, can overestimate or underestimate the necessary number of ballots required for a successful audit. In the overestimation case, the audit is inefficient and a waste of resources; in the underestimation case, the audit doesn't fulfill its purpose. That said, a fixed percentage audit is still better than no audit at all and is regarded as a "good" standard of practice.

The second type is the statistical audit where statistical methods are used to determine and inspect the minimum number of ballots required to confirm that an election has not been altered—this would be considered an "enhanced" standard of practice. As the margin of victory between the winner and loser narrows, more ballots are required to ensure an accurate audit. Typical implementations of statistical audits could require multiple rounds of ballot inspection if discrepancies are found with recounted ballots. If the statistical audit fails, a full recount of all ballots is necessary to ensure the election has not been compromised.

The following section discusses the "good" and "enhanced" audit techniques: (1) *Good:* fixed-percentage audits; (2) *Enhanced:* risk-limiting audits with two variants (a) comparison audits, and (b) ballot-polling audits.

Fixed-Percentage Audits

Fixed-percentage audits provide some evidence that results are valid. One example process: Counties indicate to the Secretary of State (or State Election Director) which machines they will use in the election, then the Secretary of State (or Election Director) randomly selects one DRE and one optical ballot scanner per county. The county must then audit a fixed percentage (e.g., 20 percent) of the ballots tallied by the optical scanner, as well as manually counting all the paper vote records produced by the DRE and comparing this number to the DRE's electronic vote count. This process ensures that, for the randomly selected machines, the pre-election logic and accuracy tests were successfully conducted, a chain-of-custody was maintained, and the devices functioned properly on election day. The weakness of a fixed-percentage audit is that specific devices, rather than the election itself, are audited. Election officials cannot be certain that the election as a whole was conducted correctly, but this may be the best available option for some counties with limited resources or technology.

Risk-Limiting Audits (Enhanced Statistical Methods)

The first step in any risk-limiting audit is setting the risk limit. Setting a 5 percent limit means that if an audit is conducted on an election that did, in fact, experience tampering, there is at most a 5 percent chance that the audit will not discover the error and at least a 95 percent chance that the audit will find the election outcome to be manipulated. The number of ballots required for a risk-limiting audit is determined by the risk limit and margin of victory. A closer election or lower limit requires more ballots to be audited. There are two types of risk-limiting audits: (1) comparison audits and (2) ballot-polling audits.

A. Comparison vs. Ballot-Polling Audits. A comparison audit involves recounting a randomly selected set of ballots and comparing those results with the original machine-recorded tabulation of those exact ballots, called the Cast Vote Records (CVRs). Comparison audits are typically recommended over ballot-polling audits for greater efficiency. Unlike a ballot-polling audit, a comparison audit requires knowing the original tabulation results of the specific ballots you are auditing (in the CVR) and comparing

discrepancies. A ballot-polling audit simply looks at the outcome of the ballots inspected. Because of this precision, comparison audits require far fewer ballots to be counted than do ballot-polling audits. However, comparison audits require specific data (machine tabulation and associated paper vote record from a given voting machine), which may be infeasible for some counties.

B. Audit Level. Audits can operate on different levels depending on the infrastructure available. A unit could be a single ballot, a batch of ballots, all the ballots processed by a machine or all the ballots in a given precinct. For a given unit, samples are typically selected randomly then the ballots within that unit are inspected. For statistical risk calculations, the larger the unit, the larger the total number of ballots that will need to be inspected to have the same risk of missing an incorrect outcome. Ballot-level comparison audits are most efficient in terms of number of ballots considered for a given margin of victory and risk limit because they spread the audit across many ballots in multiple precincts. This means this audit is more likely to find any election meddling. Batch, machine, or precinct level audits require doing a comparison audit on batches of ballots only at certain precincts. This is less likely to find election meddling and requires auditing more ballots to ensure the same level of confidence that an election outcome is true, but may be more feasible for some counties.

There has been extensive research on this issue by leading experts in the field of election auditing. The following reports can provide additional information:

"A Gentle Introduction to Risk Limiting Audits" Mark Lindeman and Philip B. Stark

"Bayesian Tabulation Audits: Explained and Extended" Ronald L. Rivest

"On the Notion of 'Software-Independence' in Voting Systems" Ronald L. Rivest and J.P. Wack

"Evidence-Based Elections" by Philip B. Stark and D.A. Wagner

External Resources Guide

There are many threats that could undermine the democratic process; fortunately, election officials are not in this alone. There are resources available that can help defend against those threats, including free ones.

Federal Support

The Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) offers a variety of services at no cost or minimal cost for states and counties. Services include:

1. Cyber Hygiene checks, which scan election and other Internet-accessible systems (such as public-facing VRDB portals) for vulnerabilities and configuration errors. DHS can also provide a report that outlines steps to address or mitigate vulnerabilities detected in the scan.
2. Risk and Vulnerability Assessments (RVAs), which involve DHS teams performing in-depth on-site analysis of a state or local election facility's internal and external networks. RVAs can include penetration testing, vulnerability scanning and testing, database and operating systems scans, Web application scanning and testing, and several other services.
3. The National Cybersecurity and Communications Integration Center (NCCIC) is a cybersecurity situational awareness, incident response, and management center that operates 24 hours a day, 7 days a week. NCCIC collaborates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to State and local governments.
4. MS-ISAC disseminates early warnings on cyber threats to state and local governments as well as security incident information and analysis through a 24-hour security operations center. MS-ISAC also provides intrusion detection.
5. Cyber Security Advisors (CSA) and Protective Security Advisors (PSA) are security professionals deployed in all 50 states to provide direct assistance, such as vulnerability assessments, and reach-back to additional government resources and capabilities.

Private Sector Support

For defending election system-related public-facing websites, Google's Project Shield and Cloudflare's Athenian Project are free services that defend websites from distributed denial of service (DDoS) attacks. Other software development firms are developing free open source software to assist states and localities in conducting risk-limiting audits. Several highly experienced cybersecurity firms also offer penetration testing and risk vulnerability assessments.

National Guard Collaboration

The National Guard is building cyber units in many states and territories. These units align with the Army and Air Force. When not performing their federal mission, these units may be available for state-specific tasking under state authorities. Several states have employed their National Guard cyber capabilities to participate in activities such as vulnerability assessments and penetration testing.

Recognizing that there are Constitutional and legal sensitivities, states interested in exploring opportunities with their National Guard units should work through their governor's office and ultimately their state's Adjutant General office. If states do not have a resident National Guard cyber capability, they can potentially partner for support with nearby states who do have this resource. In some cases, support can be provided through the Emergency Management Assistance Compact (EMAC) process, similar to other civil support capabilities. These compacts act as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance. A useful analogy is to consider National Guard support in cyberspace in a similar light as the laying of sandbags before a storm in the physical world.

What Every Election Staffer Should Know About Cybersecurity

1. **Everyone is a security official**
   Take cybersecurity seriously. Take responsibility for reducing risk, training your staff, and setting the example. Human error is the number one cause of breaches. Spear-phishing attacks and other attempts at interference can be thwarted with cybersecurity vigilance.

2. **Use two-factor authentication (2FA)**
   Use two-factor authentication for everything: official work accounts, personal email accounts, social media accounts, and any data storage services. Use a mobile app (such as Google Authenticator, Duo, or Authy) or a physical key (such as Yubikey or other U2F devices) for your second factor, not text messaging. 2FA is an extra step, but is very effective at preventing unauthorized access.

3. **Create long, strong passwords**
   Current computing capabilities can crack a seven-character password in milliseconds. For your passwords, create **`SomethingReallyLongLikeThisString`**, not something really short like **`Th1$`**. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of **`$ymB01$`**.

4. **Keep credentials secure**
   When collaborating with others, resist the temptation to share credentials to systems with them, regardless of who they are.

5. **Practice cyber hygiene**
   Follow all applicable guidance for patching and software updates. Ensure that your systems have the most updated antivirus software.

Glossary

Based on the Election Assistance Commission's Common Cybersecurity Terminology and Information Technology Terminology Glossaries

Cybersecurity Terms:

Access
Ability to make use of any information system (IS) resource.

Access control
The process of granting or denying specific requests: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities.

Advanced Persistent Threat
An adversary who possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

Asset
A major application, general support system, high impact program, physical plan, mission-critical system, personnel, equipment, or a logically related group of systems.

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Attacker
A party who acts with malicious intent to compromise an information system.

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

Backups
A copy of files and programs made to facilitate recovery if necessary.

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Blacklist
A list of entities that are blocked or denied privileges or access.

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected information.

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Critical infrastructure
System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, national public health or safety, or any combination of those matters.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Loss
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Decryption
The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Denial of Service
The prevention of authorized access to resources or the delating of time-critical operations.

Encryption
The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it. Encryption does not prevent interception, but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down. Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

Firewall
The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Hack
Unauthorized attempt or access to an information system.

Hash Function
An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Incident Response Plan
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information systems(s).

Intrusion
A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Multi-factor Authentication
Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something that identifies who you are (e.g., biometric).

Password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Phishing
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Port
The entry or exit point from a computer for connecting communications or peripheral devices.

Port scanning
Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Private key
A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key or to decrypt information which has been encrypted using the public key.

Risk analysis
The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls that are planned or in place.

Spear Phishing
A colloquial term that can be used to describe any highly targeted phishing attack.

Spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system.

Structured Query Language (SQL) injection
An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Tabletop Exercise
A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Threat
Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Unauthorized access
Any access that violates the stated security policy.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

General Information Technology Terms:

Air Gap

An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called "Sneaker Net." Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Audit

A review of a system and its controls to determine its operational status and the accuracy of its outputs. Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail

The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication

The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Blacklist

A list of URLs, domains, users, or other identifiers, that have had system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Code

n. Synonym for program or software.

v. to create or modify software.

Data destruction

The removal of data from a storage medium. Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database
A structured collection of data that includes data and metadata (data about the data). Databases are managed by database management systems. The election database stores all of the requisite information to manage election including precinct information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Download
Transferring data from a larger computer to a smaller computer or device. An EMS facilitates downloading ballot images to vote capture devices.

Dox
Publish damaging or defamatory information about an individual or organization on the Internet. One method of hacking a campaign is doxing (or doxxing).

File
A collection of related data, stored on media. Files will be identified by a system-valid filename.

Firewall
A gateway computer and its software that protects a network by filtering the traffic that passes through it. Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the Internet.

Two-factor Authentication
Authentication mechanism requiring two or more of the following: something you know (e.g., Password), something you have (e.g., Token), something that identifies who you are (e.g., biometrics).

Penetration Testing
Also called Pen Testing. An evaluation method that enables a researcher to search for vulnerabilities in a system. Election systems, such as the VR system, are periodically submitted to a Pen Test to determine their vulnerabilities to cyber attacks.

Ransomware
Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device. Election office computers should maintain high levels of cyber hygiene, including up-to-date anti- malware systems and adherence to best practices regarding managing browser and email client activities.

Social Engineering
Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech. Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software

A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer. The Election Management System (EMS) used to create election databases is software.

Spear Phishing

A targeted attack by hackers, via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors. Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Software Patches

Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes. Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise

A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning. Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Wi-Fi

Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections. Some e-Pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Election Administration Technology Terms:

Central Count Optical Scan

Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies. Central count systems lack overvote/undervote protection capabilities.

Digital Optical Scan System

Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems.

Direct Record Electronic Voting System (DRE)

A DRE system presents a ballot image to a voter, collects the voter's choices, and records those choices directly onto electronic media. DREs may be fitted with VVPAT subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction and image displays, and can hold a large number of ballot styles in multiple languages.

Election Night Reporting Systems (ENR)

A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near-real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Poll Book (EPB)

Hardware and/or software that permits election officials to review the electors list and mark voters who have been issued a ballot. Also called an e-Pollbook. E-Pollbooks can be standalone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

High-Speed Central Count Tabulation System

An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Optical Scan System (Op Scan)

A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan

Optical scan technology that permits voters to mark their paper ballots within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Risk-Limiting Audit

Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Voluntary Voting System Guidelines (VVSG)
Collection of standards that is developed and maintained by the EAC. The VVSG specifies a minimum set of performance requirements that

Voter Verified Paper Audit Trail (VVPAT)
Contemporaneous paper-based printout of voter choices on a DRE.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P