Photo by Brendan McDermid/Reuters
https://www.pbs.org/newshour/politics/fbi-warns-possible-state-election-system-hacks

APRIL 2020

STATE INNOVATION EXCHANGE

DEFENDING OUR DEMOCRACY: STATE SOLUTIONS TO STRENGTHEN ELECTION SECURITY

American elections face dire and unprecedented security threats. Ahead of the 2016 election, Russia launched a two-pronged campaign to sow chaos and doubt into our democracy. Hackers "scanned" election systems in all 50 states and attempted to breach systems in at least 21 states—exposing major weaknesses in our election infrastructure, regulations, and personnel readiness. At the same time, Russian internet trolls orchestrated a divisive, digital disinformation campaign to agitate and misdirect the American public. Threats to American election security have evolved and proliferated since 2016 as enemies experiment with new tactics and inspire new malicious actors.

Declining public confidence is perhaps the greatest risk to our democracy's health today and is a key objective of our adversaries. In a recent poll conducted for C-SPAN, 58 percent of voters expressed concern that foreign governments pose a threat to American elections, and a mere 31 percent of Americans have confidence that the government has done enough to protect elections from foreign interference. Conspiracy theories of vote rigging, often elevated by President Trump, have exacerbated negative perceptions of U.S. election integrity, particularly in the aftermath of close races, like Kentucky's 2019 gubernatorial election, or administrative bungles, like the 2020 Iowa caucus. Whether perceived or legitimate, concerns that votes will not be counted accurately could negatively impact participation and increase the chance that voters and candidates will not accept the outcome of our elections.

In the face of these threats, states have largely been left to fend for themselves. Despite efforts to secure election systems and update technology across the country, state and local officials on the frontlines of our democracy are not uniformly prepared to defend against these attacks in 2020 and beyond. Federal legislation has been introduced to improve election security—offering more funding for states, mandating post-election audits, streamlining information sharing, and imposing stronger deterrents and penalties—but these efforts have generally stalled or failed.

In the absence of a strong, coordinated response from Washington, D.C., to protect our democracy, this crisis requires bold action from the states. While no one state can combat the multi-faceted and evolving set of security challenges we face, state legislators and administrators can work together as a network and lead by example to protect our elections, inspire public confidence, and spur stronger federal action. State legislators play a critical role, and the foundation of our electoral system relies on their active, informed, and vigilant engagement in election security. Whether using their platform to draw attention to solutions, supporting administrators, or passing legislation, state lawmakers have a responsibility to help strengthen election security and protect the present and future of American democracy.

This brief aims to help state legislators meet this challenge. To connect with experts, advocates, or peer legislators advancing the solutions covered here, or to receive support on legislative research, communications, or strategy, please contact the SiX Democracy Team at **democracy@stateinnovation.org**.

This resource was developed by the State Innovation Exchange (SiX) with support, input, and resources from the Brennan Center for Justice, Center for American Progress, Common Cause, and Verified Voting. We sincerely thank our partners for their contributions to this brief, their support for state legislators, and their efforts to defend democracy.

10 STEPS
STATE LEGISLATORS CAN TAKE TO IMPROVE ELECTION SECURITY

Here are 10 actions you can take to secure our elections as a state legislator.

This list was originally produced by the Center for American Progress (CAP) in 2018. It was adapted by SiX and re-published here with CAP's permission. Contact the SiX Democracy Team (democracy@stateinnovation.org) and Jerry Parshall at CAP (jparshall@americanprogress.org) for help with any of these suggested actions.

TAKE LEGISLATIVE ACTION

1 Sponsor and/or support election security legislation in your state. In doing so, consult with election security experts who can advise legislative offices and assess proposed legislation. (We review an extensive set of policy solutions in this brief.)

2 Include election security funding in your state budget. Funding can come in the form of a lump sum or grants and should focus on improving election infrastructure; administrator training, protocols, and readiness; vendor oversight; failsafe and contingency planning; and postelection audits.

3 Hold legislative hearings on vulnerabilities and threats to election infrastructure as well as the importance of election security reforms. Invite state and local election officials, as well as election security experts, to testify.

4 Give floor speeches in your legislative chamber on the importance of election security solutions.

5 Sponsor nonbinding resolutions recognizing the threats posed by foreign nation states seeking to infiltrate and disrupt U.S. elections and the need for improvements in election security preparedness.

USE YOUR ROLE AS A LEGISLATOR TO ENGAGE WITH ELECTION OFFICIALS

6 Meet with state and local election officials. Ask them what support they need in administering elections and about any potential problems they have observed or expect for upcoming elections, in order to tailor legislation to fit specific needs. Meet with election security experts who can provide expertise on best practices.

7 Partner with other legislators to send letters to the top election official in your state. Ask what specific steps are being taken to fortify election security and prepare for potential attacks in upcoming elections, which the nation's top intelligence officials have warned are all but guaranteed. Request private briefings on these matters.

EDUCATE THE PUBLIC AND ADVOCATE FOR IMPROVING ELECTION SECURITY PREPAREDNESS

8 Use communications channels to influence coverage of the issue. For example, write op-eds and letters to the editor supporting election security reforms in your state, such as paper ballot voting systems and strong postelection audits. In doing so, you should remind the public that, in the face of threats to our democracy and elections, it is even more important that constituents participate in elections and maintain confidence in the overall integrity of the system.

9 Partner with other legislators to release joint statements on the election security needs and vulnerabilities in your states in order to apply pressure on governors to enact policy and dedicate necessary funds for the purposes of improving election security preparedness.

10 Advocate to Congress for funding and resources to fortify your state's election infrastructure. Apply pressure to members of Congress representing your state by providing details of how federal funding would benefit your state specifically.

"You should remind the public that, in the face of threats to our democracy and elections, it is even more important that constituents participate in elections and maintain confidence in the overall integrity of the system."

– Center for American Progress

Official DHS photo by Jetta Disco

POLICIES TO STRENGTHEN ELECTION SECURITY

In 2020 and beyond, state and local election officials must anticipate and prepare for sophisticated attacks on our election infrastructure. These attacks will exploit gaps in election administration protocols, hardware, and software, and are intended to sow chaos and doubt into our democracy. With legislators' support, state and local administrators must be given the resources and the mandate to safeguard election infrastructure, strengthen administration, prepare personnel, and create strong failsafes should a critical cyberattack occur.

Below, we review the following approaches to improve the "hard side" of election security:

- Updated & Secure Election Infrastructure
- Administrator Training, Protocols & Readiness
- Election Vendor Oversight & Procurement
- Failsafe & Contingency Planning
- Post-Election Audits

Remember: Legislators and state/local election administrators should team up to secure elections. Lawmakers should proactively engage administrators to understand ongoing security preparations, concerns, and needs in their states that the legislature can help address.

UPDATED & SECURE ELECTION INFRASTRUCTURE

Photo by Matt Rourke/AP Photo
https://www.nytimes.com/2019/04/24/us/politics/russia-2020-election-trump.html

Upgrading and securing our aging election infrastructure—including voter registration databases, electronic pollbooks, voting machines, counting machines, election night reporting systems, and election information websites—is perhaps the most straightforward security step states must take. Systems that are paperless and/or outdated pose a direct security risk and are susceptible to malfunctions that can disenfranchise and disquiet voters. Transitioning systems typically requires significant financial resources and lead time ahead of an election and, thankfully, since the 2016 and 2018 races many states have already undertaken significant infrastructure overhauls.

> **Note:** While outdated election systems are a concern, age is not directly correlated with security. For example, a system with paper ballots counted by a scanner is perfectly fine, even if over a decade old, as long as there is an audit of the computer tally. Security risks can be tolerated more if processes are in place to detect them and there is an ability to recover.

ELECTION INFRASTRUCTURE POLICY OPTIONS

State lawmakers can work with administrators to assess problems with election infrastructure and consider the following security solutions:

- **Eliminate Paperless Voting:** Voting machines without a paper audit trail can threaten election security and public confidence, as there is no true way to verify that ballots cast are logged as intended by voters. The inability to confirm the accuracy of a vote is especially dangerous given both real and perceived cyber threats facing our election systems. According to the Brennan Center, "nearly half of the states with paperless voting machines in 2016 will have replaced these machines by the 2020 elections." In 2020, only eight states are expected to have at least some paperless voting machines still in operation (Texas, Louisiana, Mississippi, Kansas, Tennessee, Kentucky, Indiana, and New Jersey), leaving an estimated 16 million (or 12 percent) of voters without a paper record. For sample legislation to end paperless voting, see Verified Voting's comprehensive database and the National Conference of State Legislators (NCSL) website. *(See the below note on concerns for voters with disabilities and the need to proactively reconcile security and accessibility challenges.)*

- **Make General Infrastructure Updates:** Some outdated election infrastructure poses a security risk in and of itself, and states should prioritize replacing equipment that is over a decade old. The Brennan Center for Justice estimates "that in November 2018, 34 percent of all local election jurisdictions [across 41 states] were using voting machines that were at least 10 years old as their primary polling place equipment (or as their primary tabulation equipment in all vote-by-mail jurisdictions)." To check on your state's technology, see Verified Voting's comprehensive database of polling place equipment.

- **End Electronic Ballot Return Options for Overseas Voters:** Under the federal Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), overseas military personnel and their families are allowed to receive blank ballots electronically. Some states have extended this allowance by permitting UOCAVA voters to return completed ballots by fax, email, and/or web. While access for military voters is crucial, cybersecurity and election experts across the political spectrum strongly caution against allowing subsets of voters to return ballots electronically, citing the serious threats electronic transmission poses to election integrity. More than 30 states continue to allow some form of online voting or ballot return, while others are intentionally ending the practice. A bill from the state of Washington would explicitly eliminate the return of ballots by fax and email to preserve cybersecurity (2020 Washington House Bill 2111).
- **Use the .Gov Domain Name:** State and local administrators are charged with giving voters timely and accurate information about elections, and this requires a website that is credible, visible, and secure. However, in today's dangerous misinformation and cybersecurity environment, local governments are at risk of having their election websites hacked or mimicked by bad actors seeking to confuse and disenfranchise voters. National Public Radio (NPR) and Security Magazine describe a simple, underutilized step administrators can take to mitigate this threat: use the .gov domain name. Websites with .gov signal credibility with voters, are harder to fake, and the domain is monitored by federal officials for security threats. In 2019, Ohio's Secretary of State required all counties to use either a .gov or .us address for election websites (see Ohio Secretary of State Directive 2019-08, p.5). Notably, moving election websites to a secure platform does not address misinformation by election officials themselves. States must also require local officials to update websites with sound information and promote every opportunity for voters to participate.

The Security vs. Accessibility Debate: By now, there is near consensus among cyber and election security experts that voting systems must rely on voter verified paper ballots to be resilient to cyberattacks and basic machine failures. This consensus is reflected in numerous documents published by the National Institute of Standards and Technology (NIST), the bipartisan U.S. Senate Select Intelligence Committee report on foreign interference, and the National Academies of Science, Engineering, and Medicine (NASEM).

Voter verification of paper ballots can occur through hand-marked paper ballots or ballot marking devices (BMDs), which are often used to assist voters with disabilities. With a BMD, a voter makes their candidate selections electronically (e.g. via a computer touchscreen), the device prints a paper ballot for the voter to review, and the ballot printout is cast into a scanner. While this setup is strongly preferred to paperless voting, the security and accuracy of BMDs relies on voters verifying that their ballots have been marked correctly. Preliminary results in recent research suggest that, unless prompted, voters do not catch errors made by BMDs and instead cast ballots that do not reflect their intent. Many election security experts therefore endorse using hand-marked paper ballots as the norm with the requirement that each polling station have one BMD to facilitate access for people with disabilities. However, organizations like the National Disability Rights Network (NDRN) resist this framing and oppose recommendations to use hand-marked paper as the primary mode of voting. NDRN is concerned that if BMDs are not used for all voters, poll workers will not set them up properly and that this will perpetuate serious inequities in voter access, security, and privacy for people with disabilities.

Legislators working on election security should engage in this debate thoughtfully, bring both local disability advocates and security experts into the conversation on election security, and work to advance both access and security in the near and long term. If jurisdictions opt to use BMDs for all or most people, voters must be educated on how and why to review their ballots, and election officials must create a seamless contingency plan to catch and address machine errors without delay.

Resources

- "Voting Machine Security: Where We Stand a Few Months Before the New Hampshire Primary," Brennan Center for Justice (August 2019)
- "Election Security in All 50 States: Defending America's Elections," Center for American Progress (February 2018)
- "Voter Verified Paper Record Legislation," Verified Voting
- "The Verifier - Polling Place Equipment Database," Verified Voting
- "Voting System Paper Trail Requirements," National Conference of State Legislatures
- "Cost of Counting the Vote: The Price of Upgrading Voting Systems in 43 U.S. Counties," and related press release, Public Citizen (May 2018)
- "Email and Internet Voting: The Overlooked Threat to Election Security," National Election Defense Coalition (NEDC), R Street Institute, Association for Computing Machinery US Technology Policy Committee (ACM USTPC), and Common Cause (October 2018)
- "A Threat Analysis on UOCAVA Voting Systems," National Institute of Standards and Technology (December 2008)
- "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman (2020)
- "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views," United States Senate Select Committee on Intelligence
- "New Report Identifies Steps to Secure Americans' Votes; All U.S. Elections Should Use Paper Ballots by 2020 Presidential Election; Internet Voting Should Not Be Used at This Time," National Academies of Sciences, Engineering, and Medicine (September 2018)

Photo by Seth Wenig/The Associated Press
https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/10/22/few-people-want-to-be-poll-workers-and-thats-a-problem

ADMINISTRATOR TRAINING, PROTOCOLS & READINESS

U.S. elections are managed by a large decentralized network of over 8,000 local offices and tens of thousands of state and local administrators. This decentralization simultaneously protects our elections against scaled cyber threats, while leaving local systems vulnerable to exploitation due to human error, protocol gaps, and limited resources. State and local officials are on the front lines defending our democracy and must be given strong support and guidance to safeguard our election processes.

PERSONNEL PROTOCOLS & TRAINING POLICY CONSIDERATIONS

Policymakers and administrators must work to address the "human side" of election security, including developing strong cybersecurity cultures in election offices, training personnel at all levels, and improving operations (including contingency planning, discussed in detail later on). Below are specific requirements state lawmakers and administrators can explore:

- **Mandatory cybersecurity training for election officials:** Mandatory, annual cybersecurity training can prevent human errors that expose our election systems to malicious actors. Training also helps officials at all levels view security as a critical responsibility. Illinois law requires mandatory cybersecurity training for all state employees, including election officials. Training is explicitly intended to help state employees with "detecting phishing scams, preventing spyware infections and identity theft, and preventing and responding to data breaches" (2017 Illinois House Bill 2371).

- **Election "cyber hygiene" checks:** State and local officials can undergo cyber hygiene checks, where security experts scan election hardware, software, and administrative practices for vulnerabilities. Texas now requires counties designated by the Secretary of State to conduct independent cyber hygiene checks (2019 Texas House Bill 1421). The U.S. Department of Homeland Security (DHS) also offers a wide range of services to help election officials with cybersecurity and infrastructure reviews and planning.

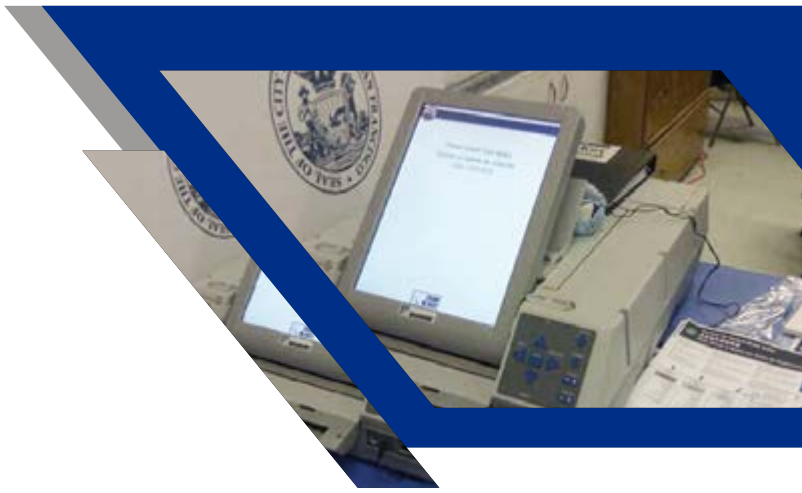
- **Incident reporting, intergovernmental communication, and escalation protocols:** State and local election officials must strengthen internal cybersecurity and communications protocols to better manage sensitive data and to improve communication and escalation procedures if a threat or vulnerability is detected. This includes communication and coordination between local, state, and federal officials. The "Election Cyber Incident Communications Coordination Guide" from the Defending Digital Democracy Project at Harvard Kennedy School offers guidance on this issue. For a state policy example, see this Indiana bill (2020 Indiana Senate Bill 380), which would require all county election officials to develop cybersecurity incident response plans. A bill from Massachusetts (2019 Massachusetts Senate Bill 1887) would have authorized an integrated state Cybersecurity Control and Review Commission, including a cross-section of officials working to secure elections, transportation, utilities, and other critical infrastructure.

According to GovTech, in 2018, Connecticut used a portion of its $5 million federal election security grant to "provide cybersecurity training to all local election officials and hire IT professionals to assess vulnerabilities within voter registration lists maintained at the local level…The state also [hired] a full-time cybersecurity consultant to work for four years to evaluate its election security and develop an incident response plan, and [allocated] $600,000 over the four years for that work."

Resources

- "The Elections Battle Staff Playbook," Defending Digital Democracy Project, Harvard Kennedy School (December 2019)
- "Election Cyber Incident Communications Coordination Guide," Defending Digital Democracy Project, Harvard Kennedy School (February 2018)
- "Election Incident Communications Plan Template," Defending Digital Democracy Project, Harvard Kennedy School (February 2018)
- "The State and Local Election Cybersecurity Playbook," Defending Digital Democracy Project, Harvard Kennedy School (February 2018)

ELECTION VENDOR OVERSIGHT & PROCUREMENT



Election technologies across the country are overwhelmingly run by private vendors. These corporations are charged with creating and maintaining our voter registration databases, voting machines, ballot scanners, electronic pollbooks, election websites, and more. Yet these vendors—charged with powering and securing our democracy—are subject to shockingly little government oversight and regulation. The Guardian writes that "private vendors have long histories of errors that affected elections, of obstructing politicians and the public from seeking information, of corruption, suspect foreign influence, false statements of security and business dishonesty." In 2018, the Federal Bureau of Investigation uncovered that Maryland's primary election vendor was heavily financed by a Russian oligarch. The results reporting app developed for the 2020 Iowa caucus was insufficiently tested by the vendor, seeding confusion and mistrust at a pivotal moment for our democracy. And while no evidence of malfeasance surfaced in either Maryland or Iowa, these kinds of connections and traditional lack of oversight are alarming and should be corrected going forward.

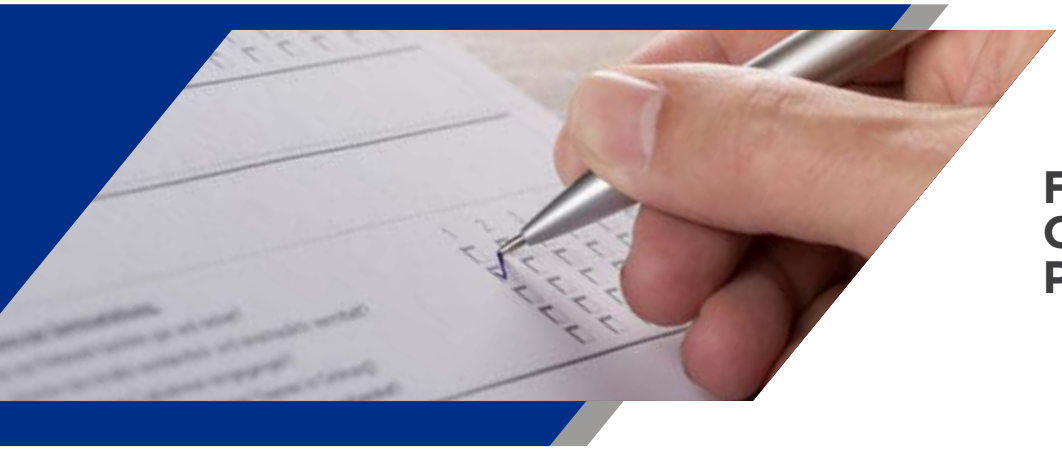
Election Vendor Oversight Policy Considerations

States should require thorough vetting of and transparency from election vendors, emphasize security requirements during the procurement process, and hold contracted companies accountable to sound security practices when providing election services. To improve oversight, state legislators may update statutes (or partner with election officials on rulemaking) to require election vendors to:

- **Disclose foreign ownership, interests, or control.** Maryland now requires election vendors to disclose any level of foreign ownership or investment, or changes in foreign interests. The state reserves the right to terminate vendor contracts if it determines that a foreign national "has the ability to control, influence, or direct the election service provider in any manner that would compromise or influence, or give the appearance of compromising or influencing, the independence and integrity of an election" (see 2019 Maryland Senate Bill 0743).
- **Disclose the source code** for election-related software, enabling independent examination and detection of security flaws (see New York Election Law § 7-208).
- **Submit timely incident reports** in the event an attempted or successful systems breach or security vulnerability is discovered. Colorado requires vendors to "submit a software or hardware incident report to the Secretary of State no later than 72 hours after a software incident has occurred." Vendors must also "notify the Secretary of State within 24 hours of a reported or actual malfunction of its voting system (see Colorado Code Regs. 1505-1:11, Rule 11.7.1 (2018)).
- **Participate in independent security assessments,** including penetration testing, where external experts attempt to compromise the election system to test its security and uncover flaws (see California Election Code §§ 19230-19233).

Resources

- "A Framework for Election Vendor Oversight," Brennan Center for Justice (November 2019)
- "A Procurement Guide for Better Election Cybersecurity," Brennan Center for Justice (August 2019): This resource includes additional examples of legislative, rulemaking, and Request for Proposal (RFP) language.
- "A Guide for Ensuring Security in Election Technology Procurements," Center for Internet Security (April 2019)
- "The State and Local Election Cybersecurity Playbook," Defending Digital Democracy Project (D3P), Belfer Center for Science and International Affairs, Harvard Kennedy School
- "'They think they are above the law': the firms that own America's voting system," The Guardian (April 2019)



FAILSAFE & CONTINGENCY PLANNING

The cybersecurity threats facing American elections are constantly evolving, and no state will ever have a system that is entirely fail-proof or secure from external actors. State and local election administrators must, therefore, create strong contingency plans in the event of a major systems malfunction, failure, or cyberattack. While prevention of election technology failures and security breaches should always be the first priority, contingency planning (including strong training, execution, and public communication) is necessary to prevent voter disenfranchisement, preserve the integrity of vote counts, and maintain public confidence.

Contingency or resiliency planning is perhaps the single-biggest step states can take in the near term to help safeguard the 2020 election process.

CONTINGENCY PLANNING POLICY CONSIDERATIONS

Election failsafe protocols are typically included in administrative rules but can be codified in statute to ensure consistent implementation across localities and in future elections. Lawmakers are encouraged to review the Brennan Center for Justice's resources on election contingency planning (Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials and the Election Security Advance Planning Checklist), connect with state/local officials about this guidance and ongoing emergency planning in the state, and assess any concerns or resource gaps that legislation could address. In particular, legislators and administrators should prepare for malfunctions and failures with:

- **Electronic pollbooks**, the systems poll workers use to verify that a voter is registered, is at the correct polling place, and has not already cast a ballot;
- **Electronic voting and counting equipment**, the machines voters use to directly cast or submit their ballots;
- **Election night reporting systems**, sites that officials use to report and publicly share unofficial election results; and
- **The voter registration database**, the statewide account of all voter information.

The following policy areas are priority failsafe measures for state lawmakers to consider:

- **Require Paper Backups of E-Pollbooks:** According to the Brennan Center, "Paper backups of e-pollbooks are the best resiliency measure in the event of an e-pollbook failure. They allow poll workers to continue confirming voters' eligibility, diminish the potential for long lines, and may minimize the need to issue provisional ballots." A Virginia bill (2020 Virginia HB 1421) would require the general registrar of each county to "produce and distribute a printed copy of the pollbook to each precinct."

- **Require Sufficient Supplies of Paper Ballots:** In states where people vote on paper ballots, polling places should have ballots on hand for 100 percent of registered voters. In states that use voting machines or ballot marking devices, polling places should be equipped with "emergency paper ballots for two to three hours of peak voting," according to the Brennan Center (Election Security Advanced Planning Checklist).
- **Strengthen Provisional Ballot Protocols and Supplies:** Provisional ballots are an important, albeit imperfect, backstop if state voter registration databases or e-pollbooks are compromised, including if voter records are altered or deleted. The Project on Government Oversight (POGO) recommends that states (1) "clarify in their provisional ballot laws that inability to confirm registered status does not invalidate provisional votes," (2) "replace discretionary review standards for counting provisional ballots with clear and objective criteria," and (3) "maintain a full contingency of provisional ballots" for all registered voters, or have a system where a large number of provisional ballots can be printed on or just before Election Day.
- **Conduct "Doomsday" Scenario Simulations:** Colorado has held "doomsday" summits where county clerks from across the state participate in election emergency scenario exercises to ensure preparedness. In other states, legislators could encourage or allocate resources for election officials to organize this kind of training for local officials.
- **Offer Election Day Registration:** Election Day registration (EDR)—a system that allows voters who present proof of identification and residency to register and vote on Election Day—is itself a strong fail-safe policy. EDR can minimize disruption, disenfranchisement, and provisional ballot use in the event of certain e-pollbook or voter registration database malfunctions. As of January 2020, 21 states and D.C. offered EDR. See Minnesota Statutes Annotated § 201.061 for an example of an EDR statute, and email SiX for additional information and policy guidance.

North Carolina E-Pollbook Malfunction: In 2016, an e-pollbook malfunction significantly delayed voting in Durham, North Carolina. E-pollbooks in multiple precincts wrongly indicated that voters had already voted, weren't registered, or required identification, but officials did not have a simple process for switching to paper backups to keep the process running. A stronger failsafe policy and consistent training for local officials would have limited harm to voters and damage to public confidence in the integrity of the process.

Resources

- "Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials," Brennan Center for Justice (December 2019)
- "Election Security Advance Planning Checklist," Brennan Center for Justice (December 2019)
- "Securing Our Elections: How States Can Mitigate the Potential Damage of Hacked Voter Registration Rolls," Project on Government Oversight (November 2018)
- "Provisional Voting," Election Assistance Commission
- "Making provisional voting easier in Virginia," Center for Civic Design
- "Millions to the Polls: Same Day Registration," Demos (February 2014)
- "Same Day Voter Registration," National Conference of State Legislators

POST-ELECTION AUDITS

https://freedom-to-tinker.com/2018/12/10/pilots-of-risk-limiting-election-audits-in-california-and-virginia/

Post-election audits are a crucial quality control and security tool in our modern election era. Audits evaluate and identify flaws in our election technology, both accidental and deliberate, and help ensure that individual ballots cast by voters are counted and tabulated correctly. Audits can also provide statistical assurance that election outcomes are trustworthy.

While many states across the country have taken steps to improve post-election auditing in recent years, there is more we can do. A 2018 assessment from the Center for American Progress found that "[33] states have post-election audit procedures that are unsatisfactory from an election security standpoint, due either to the state's use of paperless [voting] machines, which cannot be adequately audited, or other factors. At least 18 states do not legally require post-election audits or require jurisdictions to meet certain criteria before audits may be carried out." **Review CAP's profile of your state to identify gaps and opportunities to improve your post-election audit process.**

POST-ELECTION AUDIT POLICY CONSIDERATIONS

Traditional audits help administrators detect malfunctions with individual voting machines. Election officials review paper ballots (or ballot trails) cast in a set of randomly selected precincts or machines and compare paper records to electronic vote tallies. Over the last decade, various forms of traditional audits have been common practice in a majority of states. Unfortunately, these audits only spot-check machine function and do not confirm that the results of the election are correct.

Risk-limiting audits (RLAs), a newer approach, help ensure that officials declare the correct winner of an election—or "limit the risk" of declaring the wrong winner. Election officials manually tally a random sample of paper ballots and compare the sampled results to the computer-reported results. The RLA is a statistically sound way to check that the computers counted the votes properly, and it is typically less resource-intensive than traditional audits (as the number of ballots audited is only as high as needed to validate election results with statistical confidence). Increasingly, experts consider RLAs to be the gold standard method for post-election audits. RLAs tell election officials what they really want to know: "How confident are we that the winner really won?"

Risk-Limiting Audits Gain Momentum: As of January 2020, a dozen states had moved to either mandate RLAs (Colorado, Rhode Island, Virginia), authorize RLA pilot projects (Georgia, Indiana, Michigan, Nevada, New Jersey), or permit local officials to use RLAs as their post-election audit method of choice (California, Ohio, Oregon, Washington).

Ideally, post-election audits should:

- be conducted on paper ballots that voters have actually verified;
- be mandatory;
- audit a statistically random sample of ballots, machines, or precincts,
- tie the sample size of audited ballots to the electoral margin of victory (rather than auditing a fixed percentage of ballots for all elections);
- cover all categories of ballots (including regular, early, absentee, provisional, and overseas ballots);
- be accessible to the public;
- occur in a timely manner before election results are certified; and
- trigger escalation, a full recount, or a reversal of preliminary results if discrepancies are found.

Legislators do not need to resolve each of the above elements directly in bill language, but these factors should be addressed through a combination of rulemaking and statute (developed in partnership with election officials). Risk-limiting audit legislation, in particular, should not be overly prescriptive. Because RLAs are a fairly new method, enacting flexible legislation allows administrators to adapt and innovate as auditing methods and election technologies evolve. Technical processes and requirements of RLAs are best determined by election officials through rulemaking. For example, statute should not dictate the process of conducting an RLA or establish a specific risk-limit. Instead, legislation should simply "establish [RLAs] as the method for conducting a post-election tabulation audit, provide any necessary definitions, an implementation date, and how further rules, regulations, and procedures will be established." ("Knowing It's Right, Part One: A Practical Guide to Risk-Limiting Audits," see pages 12-14 for more detailed RLA policy considerations for states.)

For an example of a statute that mandates risk-limiting audits, see Colorado Revised Statutes § 1-7-515. For a sample statute that mandates post-election audits but allows local officials to choose RLAs as one of several methods, see Revised Code of Washington § 29A.60.185.

Resources

- Video: "Why Audit Elections?" Center for Technology and Civic Life (2019)
- Video: "3 Methods of Risk-Limiting Audits," Center for Technology and Civic Life (2019)
- "Why Do Audits? A Verified Voting Overview," Verified Voting
- "What is a Risk-Limiting Audit? and Risk-limiting Flowchart," Verified Voting
- "Knowing It's Right, Part One: A Practical Guide to Risk-Limiting Audits" and "Part Two Risk-Limiting Audit Implementation Workbook," Democracy Fund (May 2019)
- "The State and Local Election Cybersecurity Playbook," Defending Digital Democracy Project (D3P), Belfer Center for Science and International Affairs, Harvard Kennedy School
- "Post-Election Audits," Verified Voting
- "State Audit Laws Searchable Database" and "Post-Election Audits by Type in U.S.," Verified Voting
- "Post-Election Audits," National Conference of State Legislators
- "Risk-Limiting Audits," National Conference of State Legislators
- "Voting Machine Security: Where We Stand a Few Months Before the New Hampshire Primary," Brennan Center for Justice (August 2019)
- "Election Security in All 50 States: Defending America's Elections," Center for American Progress (February 2018)
- "Principles and Best Practices for Risk-Limiting Audits, Rev.," ElectionAudits.org (December 2018)

EXPERTS & ADDITIONAL RESOURCES

Brennan Center for Justice

- "How to Secure Elections for 2020 and Beyond" (October 2019)
- "What Does Election Security Cost?" (August 2019)
- "A Framework for Election Vendor Oversight" (November 2019)
- "Voting Machines at Risk: Where We Stand Today" (March 2019)
- "Voting Machine Security: Where We Stand a Few Months Before the New Hampshire Primary" (August 2019)
- "Securing the Nation's Voting Machines: A Toolkit for Advocates and Election Officials" (May 2018, developed with the National Election Defense Coalition)

Center for American Progress (CAP)

- "Election Security in All 50 States: Defending America's Elections" (February 2018)
- "10 Steps State Legislators Can Take to Improve Election Security" (March 2018)
- "9 Solutions to Secure America's Elections" (August 2017)

Center for Democracy and Technology (CDT)

- "Election Security"
- "Presentation: Engaging Policymakers at the State Level, Election Cybersecurity" (August 2018)
- "Making Sense of the Election Security Legislation Landscape" (June 2019)
- "Pennsylvania Is Taking Election Security Seriously" (March 2019)
- "State Progress on Election Cybersecurity" (February 2018)

Center for Technology and Civic Life (CTCL)

- "Course: Cybersecurity for Election Officials"
- "Course: Post-Election Audits"

Common Cause

- "Election Integrity"
- "Email and Internet Voting: The Overlooked Threat to Election Security" (developed with the National Election Defense Coalition)

Cyber Policy Center, Stanford University

- "Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond" (June 2019)

Defending Digital Democracy Project (D3P), Belfer Center for Science and International Affairs, Harvard Kennedy School

- "The Elections Battle Staff Playbook" (December 2019)
- "Election Cyber Incident Communications Coordination Guide" (February 2018)
- "Election Incident Communications Plan Template" (February 2018)
- "The State and Local Election Cybersecurity Playbook" (February 2018)

Democracy Fund

- "Knowing It's Right, Part One: A Practical Guide to Risk-Limiting Audits" (May 2019)
- "Knowing It's Right, Part Two: Risk-Limiting Audit Implementation Workbook" (May 2019)

National Conference of State Legislatures (NCSL)

- "Voting System Paper Trail Requirements"
- "Post-Election Audits"
- "Risk-Limiting Audits"
- "Election Security | Cybersecurity"
- "Election Security: State Policies"

Project on Government Oversight (POGO)

- "Securing Our Elections: How States Can Mitigate the Potential Damage of Hacked Voter Registration Rolls" (November 2018)

Verified Voting

- "Voter Verified Paper Record Legislation"
- "State Audit Laws Database"
- "Post-Election Audits by Type in U.S."
- "The Verifier - Polling Place Equipment Database"

ABOUT SiX

The State Innovation Exchange (SiX) is a national resource and strategy center that collaborates with state legislators to improve people's lives through transformative public policy. SiX provides legislators with on-the-ground support; creates tailored policy research, trainings, and communications guidance; and fosters collaboration between legislators—across chambers, across regions, and across state lines—and with grassroots movements.

Email helpdesk@stateinnovation.org to get connected with our staff.