canvass (n.)
Compilation of election returns and validation of the outcome that forms the basis of the official results by a political subdivision.
—U.S. Election Assistance Commission: Glossary of Key Election Terminology

Security and Elections: What Legislators Need to Know

The last time the mechanics of elections got as much scrutiny as now was in the aftermath of the 2000 election. For two months, a steady stream of news stories about election security has flowed by, each with a different twist. Are Russians purposefully creating chaos for Election Day? Will every vote be counted? Are some people voting more than once? Can a U.S. general election be rigged?

The Canvass is asking one extra question: What should legislators (and the public) worry about when it comes to election security, and what shouldn’t legislators (and the public) worry about? We turned to some of the nation’s best experts on election administration to address parts of the overall issue.

Whose job is it to run elections and to protect them?

American democracy’s greatest strength—and weakness—is the diffused nature of election administration. The ability of a determined enemy to hijack our election process is largely thwarted by the thousands of different jurisdictions administering elections pursuant to different laws, using different procedures, running on different software, all without one central, monolithic election administration authority. On the other hand, the fact that most of those different jurisdictions are underfunded, the different procedures sometimes out of date, and the different software often insecure or running in an insecure environment opens the door for localized threats.

Ideally, the current discussion on cyber-security will lead us to keep our strengths and eliminate the weaknesses. For me, that means: (1) retaining local control over election administration, with channels of oversight for each Secretary of State or equivalent; (2) while maintaining that local control, having consistent and relevant security standards throughout the country; and (3) funding to implement those standards. For too long the federal government has depended upon and enjoyed the benefits of local election administration without contributing to its success. The establishment of the U.S. Election Assistance Commission was a positive first step, in that their charge in elections is “assistance.” While it would be counter-productive and dangerous to federalize the election process, the federal government should provide meaningful assistance.

The United States sees itself as the world’s greatest democracy. As the son of a refugee who came to this country fleeing oppression, I believe that to be true. In this new interconnected world local governments, the states, and the federal government each needs to step up and protect that democracy so that we can be a shining example, and not a laboratory of what not to do.
What role does the federal government play in election security? What role should it play?

The U.S. Election Assistance Commission (EAC) is working with all levels of government and other stakeholders to support state and local election officials as they provide an accessible and secure voting process. We do this by equipping state and local election officials with EAC resources, integrating the security community in our Voluntary Voting System Guidelines drafting processes, and facilitating conversations on the security of our voting systems throughout the year. We also participate in conversations with agencies like the Department of Homeland Security and the Federal Bureau of Investigation, but it is important to remember that our efforts regarding security are year-round and ongoing.

An example is our #BeReady16 initiative. BeReady16 is a reflection of my belief that everyone, from the federal government to the local election official, plays a role in election security.

I know that many people are talking about election security, but I want to make sure that voters remain confident in our elections. I believe that our elections are secure because I have been working alongside election officials as they have been preparing for this year’s elections. I want voters to have the same confidence that I have. So, I am encouraging all voters to talk to their local election officials and to volunteer as poll workers. You will be more confident in our elections after the experience, and you will provide a great public service.

Lastly, we should take care when discussing election security. When we are not aware of credible threats to our elections, we should not take actions that might insinuate that such threats exist. Voter confidence is of the upmost importance, and conversations that are not based on credible threats and that occur too close to elections can unnecessarily reduce this confidence.

The EAC and many others continue to monitor the security of this year’s elections and are confident that they are secure. I urge all who discuss this issue to do so in an informed and responsible manner.

What safeguards are in place to protect against in-person (mostly Election Day) voting fraud?

Voter fraud in Minnesota is incredibly low—almost nonexistent. In fact the word fraud is misused and abused. Often, clerical errors caused by humans are the culprit in what some call examples of “voter fraud.” We also hear about voter fraud committed by non-citizens. But the truth from my perspective is that naturalized citizens voting for the first time take their ability to vote very seriously, and would never risk deportation for voting prior to being granted citizenship. When voter fraud has occurred in Minnesota, it usually involves felons still on probation who have not been properly informed that their voting rights are not restored until after the completion of their full sentence.

There are several safeguards we take to mitigate the opportunity for fraud on Election Day:

- Registering to vote prior to the election is validated through integrated systems such as the Department of Motor Vehicles, U.S. Postal Service, Social Security, Minnesota Office of Vital Records, etc. Minnesota now uses the Electronic Registration Information Center for added security.
- Affirming registered voter’s eligibility to vote on Election Day and requiring the voter to sign the roster attesting to their eligibility to vote as well as verifying identity and residency for those registering to vote on Election Day.
- Documenting in the roster voters who have already voted by absentee ballot to prevent double voting.
- Conducting post-election canvasses that compare voter signatures or ballot applications with the numbers of ballots cast; qualifying and counting provisional ballots in certain states; and calculating, certifying and publicly sharing official totals.
- Using technology such as e-pollbooks—which will be fully implemented in Minneapolis in 2017—to minimize human errors and safeguard against potential fraud.

One big number

49 percent. According to new research from the Pew Research Center, only about half of all registered voters (49 percent) are “very confident” that their vote will be accurately counted in the upcoming election. The polling is split by party too, with Trump supporters (38 percent) reporting far less confidence than Clinton’s (67 percent).

Overall, voters are less confident that their vote will be accurately counted in the upcoming election than they were in 2004 and 2008. In 2004, 62 percent of voters were “very confident” their vote would be accurately counted and 57 percent were in 2008.
What happened with voter registration databases in Arizona and Illinois?

Protecting voter registration information is the number one priority for my office’s cybersecurity team. That’s why we’ve been concerned with inaccurate reports regarding our voting equipment and the potential exposure of registration data. We have made a number of upgrades in Arizona’s plan for election integrity and those improvements have enhanced the security of voters’ information.

Last week the media suggested both Arizona and Illinois had suffered hacks of their voter registration systems. Those reports implied our state failed to take adequate precautions to prevent cyber-attacks. Those reports are inaccurate. Our computer security experts tell me that no unauthorized user ever got access to state voter registration information. At most someone stole a login ID of a county election worker. And, several months ago, we implemented all of the recommendations cited in those media reports to prevent this specific type of cyber-attack. But still, I worry about election integrity issues every day.

Over the next decade our state will have to develop and implement a plan to replace aging voting equipment and streamline the state’s voter data systems. We work closely and cooperatively with county election officials to ensure ballots are counted accurately. We test every vote counting machine before every election. Historically our counties have had to pay for new election equipment as they felt they needed it. So elections equipment is considered in the same context as the sheriff’s department budget or road paving allocations. I understand why lots of other things get replaced or updated before elections equipment, but the time has arrived to focus on this issue.

The attack in June failed. But that might not be the case next time. As sophisticated hackers around the globe continue to look for ways to steal our personal information, we must invest in our security and voting systems to prevent attacks before it’s too late—Arizona Secretary of State Michele Reagan.

According to Illinois State Board of Elections (SBE) official reports, Illinois was the victim of a malicious cyberattack of unknown origin against the Illinois Voter Registration System database beginning June 23, 2016. SBE staff became aware of a breach on July 12 and immediately took measures to stop the intrusion. In the following weeks, SBE staff worked with a variety of entities including the Federal Bureau of Investigation and Department of Homeland Security to determine the scope of the intrusion, secure databases and web applications, comply with state law regarding personal information loss, and assist law enforcement in their investigation.

Although the investigation is still in progress, the hackers were definitively able to view 700 files, and possibly able to view 90,000 voters’ records by compromising the passwords to the voter registration database.

“If a voter’s records were viewed, hackers could have obtained the voter’s name, address and date of birth,” said the Illinois State Board of Elections in a press release. “If the voter provided a phone number, email address, driver’s license number or the last four digits of his or her social security number when registration occurred, that information may also have been viewed. Even if a voter’s record was viewed, the Board is sure no records have been altered or changed in any way.”

What if an election is disrupted—what’s the backup plan?

In almost every election that we have, there is opportunity for some sort of disruption. In Harris County, we have encountered many, including a fire burning all of our election equipment 67 days before an election in 2010, laws changing immediately before an election, a truck knocking down a telephone poll disconnecting all of our communication between our early voting locations, loss of power at multiple polling locations and a chemical spill on Election Day. In response to these events, we did not waiver from our processes and were prepared with backup systems and support systems.

Developing solid processes that include cross-training, off-site system backups, emergency generators, and maintaining excess supplies is key to responding to any event. Alongside good processes, it is essential to work well with other county departments, know your vendors and their capacity to provide support, and develop a close relationship with the secretary of state.

One of the most vital components to success has been not deviating from well thought-out processes and delegating the non-routine jobs to those who offer assistance and allowing them do what they do best, i.e., purchase equipment, write inter-local agreements, find new locations, etc. The time taken to discuss and plan for the “what if” disruptions well before Election Day can pay dividends. Election administrators should always remember Murphy’s Law: “Anything that can go wrong, will go wrong”—Stan Stanart, Harris County Clerk and Chief Election Official, Texas.
**How do we know voting equipment counts votes correctly and how is it protected against tampering?**

Voting systems—the equipment on which votes are cast and counted—are the most investigated, most tested, and most secure systems used in the conduct of elections. Voting systems are designed to conform to the security, accessibility, and functionality standards of the federal standards known as the Voluntary Voting System Guidelines (VVSG). Before a voting system is acquired and deployed in a jurisdiction, its software, hardware, firmware and operating system are tested at the federal level by independent laboratories and at the state level by state testing authorities to ensure that every vote is captured as intended by the voter, every ballot is accurately and completely tabulated and all results are auditable. The testing of the voting system involves source code review (to ensure there is no extraneous or malicious code in the system) and the casting of hundreds of thousands of ballots to assess the accuracy and fault tolerance of the system.

**Surrounding the use of every voting system are layers of overlapping physical, logical and procedural security safeguards that check and double check that no tampering has occurred to the ballot before or after it enters the processing queue.** Local election offices must maintain meticulous records that account for every ballot ordered, issued, counted and even their eventual disposal.

Election officials, poll workers, and IT staff are trained in the proper maintenance, deployment and use of their voting systems. This training includes not only the correct procedures to prepare the equipment and ballots for the election, but also the maintenance and secure storage of the systems before, during and after the election. Election officials observe strict chain of custody rules that prevent voting system components from falling out of custody, undetected.

Every jurisdiction engages in pre-election testing, called logic and accuracy testing, of their systems and ballots. This public demonstration of the content of the ballot and the ability of the voting system to accurately and completely tabulate the ballot and report results, is an important demonstration and validation of the correctly functioning voting system.

By the time voters get to cast their ballots, that jurisdiction’s voting system has been subjected to thousands of test procedures that ensures it will faithfully capture voters’ intent, record the vote properly and tabulate it accurately and completely—Merle King, Executive Director of the Center for Election Systems, Kennesaw State University.

**We often hear, “soon we’ll be voting on our phones.” And yet, it just isn’t so. How does the internet pose a risk to secure voting?**

Every internet-connected device is constantly under attack by bad actors trying to steal information or infect machines with malware. The internet was, is, and continues to be, the wild west of cyberspace.

**Consequently, it is a very bad idea for elections systems—especially those that help cast or count votes—to be on the internet.** Whether you are voting with a computer or a smartphone or submitting a completed ballot via email, both play into the hands of those who can wreak havoc on an election.

Researchers in digital elections have been working for over 20 years on the core problems of internet voting. In particular, internet voting would need to permit someone to:

- Prove who they are and that they should be permitted to vote.
- Vote anonymously without being coerced and keep their ballot private—including being unable to prove to anyone how they voted.
- Guarantee that their vote is untampered with by malware on their own computer or by election officials receiving the vote.
- Guarantee that every legal vote is counted correctly.

After over 20 years of research by hundreds of researchers, very few in the community think that we have solved, or are about to solve, all of those core problems. We, as a whole, disagree with the assertions made by vendors selling internet voting products and services: their products do not solve all of the core problems—there are always compromises that violate fundamental principles of democratic elections. Furthermore, the security of their proprietary products is suspect. If the National Security Agency and the Office of Personnel Management can be hacked, do you seriously believe that these internet voting vendors cannot be? I have recommended that election systems must be publicly owned, transparent to all and open source, and they must be built to at least the same quality and security standards as those systems that protect our national security—Joe Kiniry, CEO and Chief Scientist, Galois.
Should Americans be worried about elections security at all?

The reason it is hard to rig an American election through a concerted conspiracy is because American elections are decentralized. American elections are decentralized because the Constitution abhors centralized control. The Founders wanted control over elections to be dispersed to the states so that no single authority could exercise control over the outcomes.

Now we are benefiting from that decentralization. Even if foreign sources are attempting to hack into election data, there is very little they could do with it. Hundreds of state and local governments house voter registration databases. That complicates the job of any hacker. Moreover, because elections are not managed from a centralized national authority, it makes it next to impossible to manipulate election outcomes. There is simply no way for an outside agent to “hack” the results of an election. Precinct level polling data isn’t connected to the internet. In most places, tally sheets are still produced by pen and paper. Too many backup records exist for any hacking effort to succeed. The idea of an election being stolen by an outside hacking attack is a fantasy.

The greater threat to our elections is the uncoordinated threat of voter fraud. States that fail to participate in multi-state compacts, such as the Kansas Crosscheck, are almost certainly allowing registrants to vote who vote in other states. Voter rolls are corrupted with millions of dead and ineligible voters. These are the bigger threats to our elections, not foreign hackers—J. Christian Adams, President, Public Interest Legal Foundation.

If there isn’t an agreement that we have a winner for the presidency or some other office, what happens next?

Procedures differ from state to state, and also for different offices. For the presidency, ultimately a joint session of Congress must confirm a winner, but a lot can happen before Congress becomes involved—as we learned in 2000. For the Senate and the House, each chamber has the constitutional power to decide which candidate to seat, or to require a new election. State legislative chambers have equivalent authority under state constitutions, and state legislatures often have the last word if an election for governor is disputed. But before a disputed election reaches a legislature, various administrative and judicial procedures can occur.

First, after the initial returns on election night, there is a canvass of those returns, to verify the initial tabulation and to determine the eligibility of any ballots not yet included in the returns. Second, if the margin of victory is close enough there may be a recount.

A candidate who is not satisfied at that point may go to state or federal court, in an effort to affect the rules and procedures used during canvass and recount proceedings. Finally, a candidate may file a judicial contest of the election, claiming that the result is incorrect because of error or fraud. And if there is reason to believe that a state court’s handling of the contest is inappropriate, a candidate can convince the federal judiciary to block the state court’s proceedings, as occurred not just in the 2000 presidential election, but also the 1994 election for Alabama’s Chief Justice (among other examples). The more a state legislature does before an election to improve the state’s procedures for handling these cases, the less likely the federal judiciary will invalidate the state’s own proceedings—Ned Foley, Director—Election Law, Moritz College of Law, Ohio State University.

What are the post-Election Day procedures states can take to confirm the election went well?

Ensuring the accuracy and integrity of the vote count can help generate public confidence in elections. Two of the most important steps happen after voting concludes on Election Day.

Ballot accounting and reconciliation (BA&R) is a not-so-exciting name for a crucial best practice. BA&R is a multi-step process that is designed to account for all ballots, whether cast at the polling place or sent in remotely, and compare that with the number of voters who voted, as the first pass. After that, the next step is to ensure that all batches of votes from all the polling places are aggregated into the totals once (and only once). This is a basic “sanity check” that makes sure no ballots are missing, none are found later, none were counted twice, etc. Most jurisdictions do a good job at this task.

Post-election audits enable verification of the voting system’s correct operation regardless of whether a voting system has malfunctioned, suffered an error in ballot programming, or been breached through malfeasance. Audits involve manually checking a representative sample of paper ballots in order to confirm that counting software has functioned correctly.

Good post-election audits are: 1) robust—examining more than just one or two contests; 2) comprehensive—including all types of ballots and voting systems; 3) timely—starting after the initial count is published and ending before results are finalized; 4) transparent and random—auditing an observably random selection of units and ensuring the count itself is observable; and 5) expandable—resolving unexplained discrepancies found in the count. Risk-limiting audits give the highest level of assurance that outcome-changing error can be found, using statistical methods to ensure greatest efficacy—Pam Smith, Executive Director, Verified Voting.
The concern about the presidential election being rigged has brought attention to previously unsung aspects of election administration. While it makes sense to focus on hacking and fraud, it’s important to remember the hard work of election administrators and poll workers across the country in preparing everything necessary to ensure millions of Americans can cast their votes with dignity and privacy. Nothing can be 100 percent foolproof on Election Day, but it is humbling to know the dedication that occurs throughout the year so we can exercise one of our most precious and fundamental rights.

We’ll be back to our regularly scheduled format next month.

Browse the most recent entries from the election team on the NCSL Blog.

Look for #NCSLelections on Twitter.

Thanks for reading, let us know your news and please stay in touch.

—Wendy Underhill, Dan Diorio and Amanda Buchanan