BRENNAN CENTER FOR JUSTICE
TWENTY YEARS
at New York University School of Law

ELECTION 2016
CONTROVERSIES

Voting System Security and Reliability Risks

The last few weeks have brought renewed attention to the security and reliability of our voting systems. After credible reports last month that Russia was attempting to influence American elections by hacking into the DNC email server and other campaign files, new reports show the FBI has determined foreign hackers penetrated two state election databases.

This fact sheet describes what the risks to America's voting system security really are — and what states, localities, and voters can do to prevent successful attacks against the integrity of our elections.

The Brennan Center has studied the use of computerized voting systems for over a decade. In a comprehensive study released last year, we found the use of outdated voting equipment across the country presents serious security and reliability challenges.

The United States has made important advances in securing our voting technology in the last few years. Relatively few votes are cast over the internet or machines connected to the internet,[1] and the vast majority of ballots will be cast on systems that have a paper trail that allows election officials to independently verify software totals. This makes it highly unlikely that a cyberattack against our voting machines could have a widespread impact on the results of a national election.

Still, there is much more we should do to promote the security and accuracy of our voting systems. Computer scientists have demonstrated that older equipment, in particular, can be very insecure. It is also more difficult to maintain, and more likely to fail (even without interference from an attacker) on Election Day. While small-scale attacks or failures of individual machines might not have a widespread impact on national vote totals, they can severely damage voter confidence, and would be particularly troubling in very close contests.

Similarly, while proper safeguards can ensure attacks on voter registration databases don't prevent a legitimate voter from casting a ballot or having her vote counted, an attack on these systems could put voters' personal information at risk. Election officials must take all steps necessary to protect such information.

In the short run, we should do everything we can to minimize the impact of such attacks or failures. In the long run, we must treat our election infrastructure like other critical infrastructure, with regular investments and upgrades.

***

[1] Several states allow military and overseas voters to cast ballots by fax, e-mail or internet portal. Alaska allows any qualified voter to request and return an absentee ballot via facsimile.

Before detailing how election security and reliability can be improved, it is important to understand the significant steps that have been taken to protect the integrity of our elections over the last several years.

Improvements to Election Security

- Today, 47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines. This process includes much more rigorous security testing than previously existed.
- While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet.
- In recent years, voting machines that could be accessed remotely have been taken out of service,[2] making widespread, remote attacks much more difficult.
- Many jurisdictions have replaced their paperless machines with systems that scan paper ballots filled out by voters, or produce a paper trail that can be reviewed by the voter.
- This November, at least 80 percent of registered voters will make selections on a paper ballot, or vote on an electronic machine that produces a paper trail.

Despite these advances, there is still more work to do to ensure that all voting machines are as secure and reliable as possible.

Outdated Voting Machines Pose Serious Reliability and Security Risks

- In November, 42 states will use voting machines that are at least 10 years old. This is perilously close to the end of most machines' expected lifespan. Using aging voting equipment increases the risk of failures and crashes — which can lead to long lines and lost votes.
- Aging voting systems use outdated hardware and software. For this reason, replacement parts for older voting systems can be difficult, if not impossible, to find. Aging systems also rely on unsupported software, like Windows XP and 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.
- While nearly all of today's voting machines go through a federal certification and testing program, many jurisdictions purchased voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.
- In November, some voters in 14 states will vote on paperless electronic voting machines. These machines do not produce a paper record that can be reviewed by the voter, and allow election officials and the public to confirm electronic vote totals.[3]
- While the need for more up-to-date, secure and reliable voting equipment is clear, funders at the state and federal level seem unconcerned about our aging voting infrastructure. In at least 31 states, election jurisdictions will need new machines in the next five years, but officials from 22 of those states said they did not know how they would pay for them.

---

[2] For instance, in 2015 Virginia decertified a voting system after finding that an external party could access its wireless features to "record voting data or inject malicious data." That system had been eliminated in Pennsylvania in 2007 and Mississippi in 2013, and is no longer in use anywhere in the United States.

[3] Delaware, Georgia, Louisiana, New Jersey and South Carolina use paperless electronic voting machines as their primary polling place equipment statewide. In Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, Texas, and Virginia, some portion of polling places use such paperless machines as the primary equipment.

Short Term Solutions: Voters and Local Election Officials Can Enhance Security and Reliability

- Voters should vote early when possible, to avoid potential delays caused by machine breakdowns on Election Day.
- If voters experience problems while voting on machines, or if those machines fail, they should immediately report the problem to local officials or poll workers, and then call 866-OUR-VOTE, the Election Protection hotline, to report the problem.
- Election officials should report machine problems to the EAC so other jurisdictions using the same voting system are aware of potential issues.
- All state and local election officials should ensure the physical security of voting equipment and paper records at all stages of the process — whether in storage, in transit to polling places, or during an election — by implementing strong chain of custody procedures.
- All local election officials should conduct thorough pre-election testing on every voting machine and ensure emergency paper ballots are available at all places where electronic machines are used.
- All states should mandate thorough post-election audits to confirm that paper records match electronic results. Officials should also review and, where necessary, improve "reconciliation policies" to guarantee that the number of signed-in voters matches ballot totals, and that machine and polling place totals match county and state totals.

Long Term Solutions: State and Federal Action for Improving Security and Reliability

- Congress and state legislatures need to allocate the funds for new, reliable, and secure voting systems. Grants to fund voting technology improvements can ensure more secure voting systems for decades to come.
- Congress and state legislatures should require audits of election results, using paper ballots or voter verifiable paper records, to confirm electronic totals. Today, only 25 states require that election officials conduct paper audits.
- The next president and Congress must ensure the EAC has a full slate of commissioners and fill any vacancies in a timely manner. The work of the agency is critical to ensuring that local and state election officials have the best information to ensure our voting machines are secure and accurate.

Protecting the Integrity of Voter Registration Databases

- As long as states and local jurisdictions keep backups, including paper copies of their registration lists, no manipulation of state computer registration databases should prevent legitimate voters from casting a ballot, or having their votes counted.
- Voter registration databases can and should be programmed to run frequent, automated scans of registration activity to monitor for and alert election officials to potentially fraudulent or abnormal activity, such as a high volume of traffic or oddly timed traffic.
- Voter registration databases should be constructed to record transaction logs for all requests submitted to the site. This would allow officials to trace suspicious activity, or review activity after-the-fact for abnormal site traffic patterns.

- Websites providing online voter registration should employ best practices to protect against large-scale attacks, such as forcing an application to "time out" automatically after a certain period of inactivity, and using CAPTCHA tests.
- Voter registration databases should not contain any information other than what's required to register, or specified information relevant to the administration of elections.
- States should publish — and enforce — a policy detailing use limitations (including user authorizations) and security safeguards to protect voters' personal information in the data transfer process, the online or telephone interface, and the maintenance of the voter registration database.