Center for American Progress

Election Infrastructure: Vulnerabilities and Solutions

September 11, 2017

For more information on vulnerabilities in election infrastructure and common-sense solutions, read the Center for American Progress' "9 Solutions to Secure America's Elections."[1]

In June 2017, the American people learned that Russian operatives had targeted 39 state election systems in the lead-up to the 2016 elections.[2] Beyond the states, Russians targeted an election equipment vendor.[3] These cyberintrusions and other Election Day disruptions exposed the country's voting infrastructure as outdated and vulnerable to attack, weakening confidence in the electoral process. One poll found that 1 in 4 Americans will consider abstaining from voting in future elections due to concerns over cybersecurity.[4] Election officials at all levels of government must invest in America's election infrastructure and defend the security of our election system.

Outdated voting machines are vulnerable to cyberintrusions and system failure

- An estimated 42 states use voting machines that are more than a decade old. This is beyond the predicted 10-year life span of most models.[5]

- Outdated voting machines pose serious security risks and are susceptible to system crashes, "vote flipping," and hacking, as many rely on outdated computer operating systems that do not accommodate modern-day cybersecurity protections.[6] Moreover, upkeep for outdated machines is becoming increasingly difficult, since many parts are no longer manufactured.[7] Studies have shown how easy it is to hack election machines.[8]

- Election administrators should replace and upgrade all voting machines and components that still use outdated operating systems to new models that meet modern standards and up-to-date cybersecurity protections.

Voter registration systems are prone to hacking

- Last year, hackers breached voter registration databases in Illinois, compromising the voting records of as many as 90,000 people.[9]

- The U.S. Department of Homeland Security (DHS) found that Russian cyber actors specifically targeted voter registration databases before the 2016 elections.[10]

- Voter registration systems and equipment—including e-poll books—contain sensitive information, such as eligible voters' political affiliations, partial Social Security numbers, and driver's license numbers.[11] If voter registration records are hacked and altered, eligible Americans may be turned away at the polls or prevented from casting ballots that count on Election Day.

- Election administrators must update and secure voter registration lists and e-poll books. Paper copies of voter registration lists must be made available at each polling location in order to ensure that eligible Americans are able to cast ballots that count when they show up to the polls. In addition, states should establish contingency plans with clear guidance for election officials and poll workers on switching to paper back-ups when problems arise.

The lack of verified paper ballots or records puts election outcomes at risk

- Thirteen states employ electronic voting machines that fail to produce paper ballots or records, making robust postelection audits, or "double checks," impossible to conduct.[12]

- In 2016, some 20 percent of registered voters cast votes without leaving any voter-verified paper ballot or record—a number significantly larger than the margin of victory needed to swing the election.[13]

- Voter-verifiable paper ballots or records are necessary for conducting meaningful postelection audits that confirm election outcomes and detect malicious activity. Paperless touch-screen voting systems should be replaced with paper ballots and optical scanners.

- Voting systems that use electronic machines are often costlier because they require more equipment.[14] Each precinct, for example, requires several electronic voting machines to ensure that polling places can accommodate multiple voters at once.[15] In contrast, paper-ballot voting systems require as few as one optical scanner and one ballot-marking station per precinct to assist voters with disabilities or language barriers.[16]

Cybersecurity standards are needed to protect election infrastructure

- While many states already have some form of cybersecurity incident and disruption response plan in place to protect against and respond to cyberthreats generally, few have standards designed specifically for protecting election systems.[17]

- A security failure in Georgia's voter registration database, first discovered in August 2016, left the voter registration records of up to 6.7 million people vulnerable to outside infiltration and potential manipulation.[18]

- Local election officials should receive cybersecurity training to identify and deter election security risks. These hardworking individuals are on the front lines of our elections and are often targeted by spear-phishing attempts and other malicious activity.[19] A survey of Pennsylvania counties found that only 8 of the 42 counties that responded said their workers received cybersecurity training.[20]

- States and localities must implement cybersecurity standards for voting machines, voter registration systems, and training programs for election officials.

Postelection audits must be conducted to confirm election outcomes

- Because all voting machines are vulnerable to hacking and even misprogramming, it is of the utmost importance that election officials commit to conducting robust audits after every election in order to confirm election outcomes and to detect manipulation of vote totals.

- Conducting postelection audits is critical for ensuring confidence in election outcomes. Currently, only New Mexico and Colorado have audit processes "robust enough to detect cyberattacks."[21]

- By selecting an initial sample of ballots and interpreting them by hand, then determining whether the audit must expand, "risk-limiting" audits offer election administrators an efficient and effective way to test the accuracy of their elections without breaking the bank.[22]

Conducting tests on voting machines and equipment before elections can help mitigate risks

- While most states already have laws in place requiring state officials to test voting machines and equipment leading up to an election, their scope varies depending on the jurisdiction.[23]

- Testing should be conducted on all election machines and equipment prior to the start of early voting and Election Day, performed enough in advance to allow for effective remediation. Furthermore, testing should take place in a public forum with appropriate public notice, thereby increasing transparency and public confidence.

- In addition to conducting tests on voting machines and equipment prior to an election, vulnerability assessments—including regular system penetration testing and vulnerability scans of election infrastructure—should be required by law. In some states, the National Guard has been employed to conduct cybersecurity testing on public networks and election systems.[24]

- It is important to remember that pre-Election Day voting machine testing is not foolproof. Sophisticated hackers can manipulate pre-election testing procedures by installing malware that remains inactive during pre-election tests but activates during voting periods.[25]

Transmitting ballots over the internet poses security risks

- While most states only allow online voting for military personnel and U.S. citizens living abroad, some states—such as Alaska—allow all absentee voters to submit ballots over the internet.[26]

- Submitting ballots online is risky because there is no way for voters to confirm that the vote they cast is the same as that ultimately recorded..

- An official from DHS' Cyber Security Division warned "that online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results."[27] The National Institute of Standards and Technology has also warned against online voting.[28]

Officials across all levels of government must work together to detect and address cyberthreats

- While it is important for states to retain a level of autonomy over the administration of their elections, many lack the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cyber vulnerabilities.

- Federal agencies with expertise in cybersecurity should be responsible for carrying out comprehensive threat assessments on election infrastructure. Some states have already sought assistance in securing their election systems. Before the 2016 elections, 33 states and 36 localities requested assessments of their voting systems by DHS.[29]

- State officials—who are more familiar with the intricacies of their local systems—and federal agencies must work together to protect the security of our elections. By combining their expertise on cybersecurity threats and insight into the unique qualities of localized election infrastructure, they can better assess and deter attempts at electoral disruption.

Funding is needed to improve election security

- The cost of updating outdated voting machines across the country is estimated at approximately $1 billion, while the cost of replacing the country's paperless machines is projected to be somewhere between $130 million and $400 million.[30] Conducting nationwide threat assessments for voter registration databases is estimated to cost between $1 million and $5 million annually.[31]

- According to one study conducted by the Brennan Center for Justice, of the 274 election officials surveyed in 28 states, more than half said that they will need new voting machines by 2020.[32] Unfortunately, 80 percent of those officials said they did not have the necessary funds.

- The federal government and Congress have a duty to allocate funding, to assist in the implementation of these protective measures, and to guard against disruptions in future elections—at the very least in federal elections. This would not be the first time Congress provided funds to upgrade election infrastructure. After the 2000 presidential election, it passed the Help America Vote Act of 2002, providing more than $3 billion to help states upgrade to high-tech voting machines, among other things.[33]

Endnotes

[1] Danielle Root and Liz Kennedy, "9 Solutions to Secure America's Elections" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/.

[2] Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[3] Matthew Cole and others, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept*, June 5, 2017, available at https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

[4] Joe Uchill, "One in four will consider not voting in elections due to cybersecurity," *The Hill*, July 12, 2017, available at http://thehill.com/policy/cybersecurity/341608-one-in-four-will-consider-not-voting-in-elections-due-to-cybersecurity.

[5] Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk" (New York: Brennan Center for Justice, 2015), available at https://www.brennancenter.org/publication/americas-voting-machines-risk; Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference" (New York: Brennan Center for Justice, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[6] Pam Fessler, "Some Machines Are Flipping Votes, But That Doesn't Mean They're Rigged," NPR, October 26, 2016, available at http://www.npr.org/2016/10/26/499450796/some-machines-are-flipping-votes-but-that-doesnt-mean-theyre-rigged.

[7] Lauren Smiley, "America's Voting Machines Are a Disaster in the Making," *The New Republic*, October 19, 2016, available at https://newrepublic.com/article/137115/americas-voting-machines-disaster-making.

[8] J. Alex Halderman, "Want to Know if the Election was Hacked? Look at the Ballots," Medium, November 23, 2016, available at https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba.

[9] Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known."

[10] Jeremy Herb, "First on CNN: 33 states, 36 localities asked DHS for help protecting election systems," CNN, August 2, 2017, available at http://www.cnn.com/2017/08/02/politics/cyber-hacking-russia-states/index.html.

[11] Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known."

[12] Norden and Vandewalker, "Securing Elections From Foreign Interference"; Eric Geller, "Virginia bars voting machines considered top hacking target," Politico, September 8, 2017, available at http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492.

[13] Norden and Vandewalker, "Securing Elections From Foreign Interference." See Tim Meko, Denise Lu, and Lazaro Gamio, "HowTrump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016, available at https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

[14] Save Our Votes, "Cost Analysis of Maryland's Electronic Voting System" (2008), available at http://www.saveourvotes.org/legislation/packet/08-costs-mdvotingsystem.pdf.

[15] Sarah Breitenbach, "Aging Voting Machines Cost Local, State Governments," The Pew Charitable Trusts, March 2, 2016, available at http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments.

[16] Ibid.

[17] National Governors Associations, "Meet the Threat: States Confront the Cyber Challenge—Memo on State Cybersecurity Response Plans," available at https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf (last accessed July 2017).

[18] Kim Zetter, "Will the Georgia Special Election Get Hacked?", *Politico*, June 14, 2017, available at http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255.

[19] Cole and others, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election."

[20] Likhitha Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training," NBC News, August 23, 2017, available at https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

[21] Eric Geller, "Colorado to require advanced post-election audits," *Politico*, July 17, 2017, available at http://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

[22] See Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security and Privacy*, March 2012, available at https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[23] Jay Bagga and others, "Pre-election Logic and Accuracy Testing and Post-Election Audit Initiative" (Washington: Election Assistance Commission, 2013), available at https://www.eac.gov/assets/1/28/EAC%20Ball%20State%20Indiana%20Final%20Report.pdf.

[24] Rene Marsh, "Ohio taps National Guard to defend election system from hackers," CNN, November 1, 2016, available at http://www.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html; National Governors Association, "Act and Adjust: A Call to Action for Governors for Cybersecurity" (2013), available at https://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf.

[25] Halderman, "Want to Know if the Election was Hacked? Look at the Ballots."

[26] Sari Horwitz, "More than 30 states offer online voting, but experts warn it isn't secure," *The Washington Post*, May 17, 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/?utm_term=.4578e3410873; National Conference of State Legislatures, "Electronic Transmission of Ballots," January 16, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

[27] Horwitz, "More than 30 states offer online voting, but experts warn it isn't secure."

[28] National Institute of Standards and Technology, "NIST Activities on UOCAVA Voting," available at https://www.nist.gov/itl/voting/nist-activities-uocava-voting (last accessed September 2017).

[29] Herb, "First on CNN: 33 states, 36 localities asked DHS for help protecting election systems."

[30] Lawrence Norden and Christopher Famighetti, "Now Is the Time to Replace Our Decrepit Voting Machines," Brennan Center for Justice blog, November 17, 2016, available at https://www.brennancenter.org/blog/now-time-replace-our-decrepit-voting-machines; Norden and Vandewalker, "Securing Elections From Foreign Interference."

[31] Norden and Vandewalker, "Securing Elections From Foreign Interference."

[32] Christopher Famighetti, "How to Protect Against Foreign Interference in Elections? Upgrade Voting Technology," Brennan Center for Justice, March 27, 2017, available at https://www.brennancenter.org/How-to-Protect-Against-Foreign-Interference-in-Elections-Upgrade-Voting-Technology.

[33] *Help America Vote Act of 2002*, Public Law 252, 107th Cong., 2d sess. (October 29, 2002), available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf; Arthur L. Burris and Eric A. Fischer, "The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election" (Washington: Congressional Research Service, 2016), available at https://fas.org/sgp/crs/misc/RS20898.pdf; Legal Information Institute, "Help America Vote Act of 2002 (HAVA): an overview," available at https://www.law.cornell.edu/background/HAVA.html (last accessed July 2017).