Kansas Legislative Research Department

Katelin Neikirk
Research Analyst
785-296-3181
Katelin.Neikirk@klrd.ks.gov

State and Local Government

H-3 Election Security

In September 2017, the federal government informed election officials in 21* states that hackers had targeted their voting systems before the 2016 election.[1] Hackers also sent over 100 phishing+ e-mails to local election officials just before the election. In the summer of 2017, CNN reported hackers at a Las Vegas convention were able to breach all 25 pieces of election voting equipment present.[2] While it does not appear that information was tampered with in any state during the 2016 elections, the widespread nature of the attempts and the ease with which voting equipment was compromised during the Las Vegas convention has raised concerns.

Involving 542Δ federal elected officials and more than 18,000 state elected officials and 500,000 local elected officials, there are thousands of elections across the United States every year. This article will examine the major election vulnerabilities and how to address these issues. It also summarizes election security activities in Kansas and other selected states.

Tools Used in Elections

The many tools used in elections include voter registration data, electronic poll books, poll workers, storage and tallying of ballots, and voting devices. Due to a majority of election tools being electronic, cybersecurity and tampering are major issues concerning election security.

Voter registration data. There are two main ways in which to register to vote: filling out a form either at an authorized location or by mail, and online. Currently, 36 states, including **Kansas**, and the District of Columbia offer online registration.[3] During the 2016 presidential election, Arizona's voter registration system was breached by hackers *via* an election official's stolen username and password.[4] Illinois faced a similar situation where hackers were able to access voter registration records.[5] In both cases, there is no evidence any information was altered or deleted. The National Conference of State Legislatures (NCSL) cited several approaches used to ensure security, including registrants providing their driver's license number or last four digits of their Social Security number; automatic "time outs" after a certain period of inactivity; "captcha" boxes, where registrants must decode images that a computer

cannot decode; data encryption; highlighting unusual activity; and multi-screen systems, which offer one question on a screen.

Electronic poll books. In January 2014, the Presidential Commission on Election Administration recommended jurisdictions transition to electronic poll books (EPBs).[6] As of March 2017, NCSL noted that 30 states, including **Kansas**, permit the use of EPBs in some form.[7] EPBs replace paper poll books and allow poll workers to access the list of eligible voters, check in voters more efficiently, and prevent voters from checking in more than once. They are electronically connected to a central registration database. However, the Congressional Research Service notes there are no accepted technical standards and there are concerns about security and fraud prevention, especially for those connected to remote computers *via* the Internet. Some ways in which EPBs can be secured include use of secure sockets layer security or use of a virtual private network.

Poll workers. An Election Assistance Commission (EAC) 50-state survey of requirements for poll workers states that in all states and territories, poll workers must be at least 18 years old (with some exceptions); be registered to vote in that state; and be a resident of the county or district in which they will work, though some states have broader restrictions.[8] A majority of states, including **Kansas**, require poll workers to be trained, but the type, frequency, intensity, and requirements for who is trained varies greatly. In **Kansas** and many other places, there are no requirements for poll workers to submit to and pass ground checks or participate in other extensive vetting procedures. According to the Institute for Critical Infrastructure Technology (ICIT), many voting devices are stored in locations with minimal security, allowing relatively easy and unregulated access to alter or manipulate devices. Other potential security issues for poll workers are phishing e-mails, malware disguised as system patches, or the creation of unintentional gaps in cyber security, physical security, or both.

Storage and tallying of ballots. While paper ballots are stored in physical ballot boxes, electronic ballots are stored on device smart cards, a device's random-access memory, or other tools. Security measures limit access to the stored ballots, such as passwords, specific access cards, encryption, and tamper-resistant tape. However, there are ways to circumvent these measures, such as malware introduced into the device.

Manipulation can also occur after the ballot storage has been removed from the device to be tallied. Ballots may be tallied at the polling place or at a central location. If ballots need to be transferred to a central location to be tallied, they are transmitted *via* a network connection or the printed record or memory card is transported to the central location. Paper ballots are tallied by hand or by a scanner that produces a print-out of the votes. Voting devices that do not utilize paper ballots tally votes internally and produce either a printed or digital tally. It is estimated only 5.0 percent of ballots in the United States were tallied by hand; the other 95.0 percent are tallied either by the voting device or scanners.[9] Voting devices and scanners can create issues such as not calculating the votes correctly, or not reading or multiple readings of the same ballot. Tallying by hand carries the lowest risk for manipulation as it would be difficult to alter, switch, or destroy ballots without being caught. However, there is still the possibility of human error.

Voting devices. Voluntary technical standards for computer-based voting devices were first developed in the 1980s, but the 2002 federal Help America Vote Act (HAVA) (Pub. L. No. 107-252, 116 Stat. 1666 (2002), 42 USC 15301 et seq.) codified the development and required regular updating of standards by the EAC. Most states, including **Kansas**, require their devices conform to EAC guidelines. Under HAVA, states were granted almost $3.3 billion to upgrade voting devices.

Optical scan device. While paper ballots may still be counted by hand in a small percentage of voting jurisdictions, the most widely used device is the optical scan device, which is used in 80.0 percent of states' polling places and by all states for absentee or mail-in voting. Voters mark choices on paper ballots by hand or using an electronic ballot marking device (BMD) and the ballots are

read by an electronic counting device. Optical scan devices are regarded as more secure due to the fact that voters' paper ballots can be verified and cannot be altered electronically. If the voter does not mark a paper ballot directly, the process where an individual can verify the information printed on the paper ballot is the same as what was entered into the computer is also known as a voter verifiable paper audit trail (VVPAT). Since these devices typically use electronic devices to count ballots, vote counts are still vulnerable to cyberattacks, though an audit of the paper ballots is likely to catch any irregularities.

Direct recording electronic device. The second most utilized option is the direct recording electronic device (DRE), where voters mark choices *via* a computer interface and the voting device records them directly to an electronic memory. Delaware, Georgia, Louisiana, New Jersey, and South Carolina all exclusively used DREs with no paper trail in the 2016 election.[10] DRE devices pose a unique issue in that there is no way to verify the choice a voter intended to make is the same as the choice recorded in the device's memory. To solve this problem, many states configured the DRE devices to produce a verifiable paper record of the voter's ballot. However, a voter must review this ballot before casting it.

Limited life cycles. The average life span of electronic voting devices is less than ten years and many of the current devices in use are close to or have recently surpassed this point. Out-of-date devices and systems are not only more susceptible to technical issues, but also to cyberattacks or other means of tampering. The ICIT noted many voting devices have not been patched for almost a decade and use antiquated software that is unsupported by the manufacturer.[11] The Brennan Center estimates that the initial cost of replacing voting equipment throughout the United States could exceed $1.0 billion.[12] However, many jurisdictions do not have the funds to replace outdated technology. **Kansas** statutes place responsibility for voting devices with the counties.

Uniform voting systems. As of 2016, 18 states had statewide uniform voting devices, according to NCSL.[13] Using the same equipment in every jurisdiction in a state can be cost-effective and efficient, but it does pose some risks. The main disadvantage is all jurisdictions would be subject to the same vulnerabilities. This uniformity also creates a lack of flexibility if a problem does arise. A state would need to replace or repair all voting devices instead of just a few, creating a potential funding issue. Kansas does not have this issue, as the state uses a mixture of voting devices. Using a variety of voting devices, while typically more expensive, can lower the risk and impact of an attack. It would also mean replacing only a few devices at a time should a problem be discovered.

National Election Security

Background. Election security began to be a concern as early as the late 1800s in the United States, due in large part to widespread voting irregularities±.[14] Tools such as early voting devices, voter registration, and secret ballots provided by local election officials were all introduced during this period.

The 1970s saw increased national attention on election administration and security. Under the Federal Election Campaign Act of 1971 (FECA, Pub. L. 92–225, 86 Stat. 3 (1972) 52 USC § 30101 et seq.), Congress created a national Clearinghouse for Information on the Administration of Elections in an effort to facilitate exchange of information on election practices and procedures. In 1975, this function was transferred from the General Accounting Office to the Federal Election Commission (FEC) by the FECA Amendments of 1974 (FECA Pub. L. 93-443, 88 Stat. 1263 (1974) 2 USC 431).

HAVA, enacted in 2002, addressed improvements to voting systems and voter access that were identified following the 2000 election. Section 803 of HAVA transferred the functions of the FEC's Clearinghouse to an Election Assistance Commission (EAC). HAVA states the EAC shall serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of federal elections.

Current activities. The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) helps stakeholders in federal departments and agencies, state and local governments, and the private sector manage their cybersecurity risks. The NCCIC works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide threat and vulnerability information to state and local officials; all states are members. The MS-ISAC composition is restricted to state and local government entities. It has representatives co-located with the NCCIC to enable collaboration and access to information and services for state chief information officers. During the 2016 election cycle, the National Protection and Programs Directorate (NPPD) within DHS offered voluntary assistance from the NCCIC to state and local election officials and authorities interested in securing their infrastructure. The then-Homeland Security Secretary told a Senate hearing that 18 states accepted DHS' offer to help improve cybersecurity of their election systems prior to the 2016 election.[15] Eleven states, including **Kansas,** chose not to accept DHS' offer, citing concerns with federal intrusion on state elections.[16]

The Secretary of Homeland Security determined on January 6, 2017, that election infrastructure should be designated as a critical infrastructure sub-sector.[17] Participation in the sub-sector would be voluntary and would not grant federal regulatory authority. Elections would continue to be governed by state and local officials, but with additional effort by the federal government to provide voluntary security assistance. DHS is also attempting to obtain security clearances for the top election official in each state so they will have access to classified intelligence about cybersecurity threats.

The EAC adopted the Voluntary Voting Systems Guidelines (VVSG) Version 2.0 in September 2017. The VVSG Version 2.0 states a voting device must produce a VVPAT and the software or hardware cannot produce errors that could lead to undetectable changes in tallies.[18]

Kansas Election Security Activities

With many elections on the horizon, it is important to understand the state of election security in **Kansas.**

Voter registration. According to the Kansas Director of Elections with the Kansas Secretary of State's Office, **Kansas** utilizes the same software vendor as Arizona for the state's voter registration database. However, **Kansas** has at least one significant layer of security above that of Arizona's system.[19]

Electronic poll books. Currently, 16 counties use EPBs, though neither state statutes nor regulations provide guidance on their use.[20]

Poll workers. Poll workers must be residents of the area in which they will serve; 18 years of age, though they may be as young as 16 years old, if they meet certain other requirements; and a registered voter. **Kansas** does not require poll workers to submit to a ground examination.

Voting devices. In the 2016 election, data from Verified Voting showed that 70 Kansas counties used paper ballots; 15 used both paper ballot and DREs without VVPAT; 15 used DREs without VVPAT; and 5 used DREs with VVPAT.[21]

Statutes concerning electronic voting devices can be found in KSA 25-4401 through KSA 25-4416, also known as The Electronic and Electromechanical Voting Systems Act. **Kansas** requires voting devices to be compliant with HAVA voting system standards (KSA 25-4406(k)). County commissioners and the county election officer may select the type of voting device utilized in their voting locations, as long as it has been approved by the Secretary of State.

The Secretary of State and the Kansas County Clerks and Election Officials Association have implemented a voting system security policy:

- The voting system should not be connected to any network or the Internet;
- Strict requirements exist concerning who has access to what components;

- Election results cannot be transmitted *via* modem, network, or any other electronic form, except *via* secure electronic means;
- Before any election, voting devices must undergo system diagnostics; and
- Election equipment should be stored in a locked room when not in use.[22]

In January 2016, the Kansas Secretary of State proposed a plan to require precincts or districts to have their voting equipment manually audited by bipartisan election boards after election day and before the vote is certified by county officials, beginning in 2017.[23] He also encouraged the use of voting devices that produce a paper trail. The Kansas House of Representatives passed a similar bill, HB 2333, during the 2017 Legislative Session. The bill would require manual audits of elections and amend law related to the timing of the election canvasses and electronic voting machines. However, the Senate did not pass the bill, choosing to re-refer it to the Committee on Ethics, Elections and Local Government.

Notable State Election Security Activity

Georgia

In June 2017, a judge dismissed a lawsuit to require use of paper ballots in the June 20 congressional special election.[24] (Curling v. State of Georgia, No. 2017CV290630 (Georgia Superior Court, filed Jun. 9, 2017)). Plaintiffs stated voting devices were uncertified, unsafe, and inaccurate and that the Center for Election Systems at Kennesaw State University, which runs the equipment for the entire State of Georgia, is risking malfunction and intrusion. On June 30, 2017, a bipartisan group of voters filed a separate suit against the State over the same special election, citing similar reasons.[25] Plaintiffs in both cases want the state to switch to the paper ballot system, which can be audited.

New Jersey

New Jersey was one of two states that held a statewide election in November 2017, the first statewide elections since the hacking attempts during the 2016 presidential election. A bill (2017 A-4619) was introduced in the New Jersey Assembly to require voting devices purchased or leased following the bill's effective date to produce a permanent paper record.[26] Under current law, the requirement for the purchase of new voting machines or retrofitting of existing voting devices to produce a paper record has been suspended until funding is made available. The bill also would delete a provision that allows the New Jersey Secretary of State to grant a waiver from the requirement to purchase new voting devices or retrofit all existing voting devices. The bill was referred to the Assembly Judiciary Committee, with no further action taken as of November 2017.

Ohio

Legislators in Ohio have proposed a bill (2017 SB 135) to help fund the purchase of new voting devices.[27] The bill would have the State pay 80.0 percent of the costs and the counties would pay the remaining 20.0 percent. The funding request would total $89.0 million for voting devices, including $7.0 million to reimburse counties that have already done full or partial replacements.[28] The bill, as of November 2017, is in the Senate Finance Committee.

Virginia

Virginia also held a statewide election in November 2017. In September 2017, the Virginia Board of Elections (Board) ordered 22 counties and towns to adopt all new paper-ed voting devices before November.[29] Local election authorities were responsible for the associated costs. The Board de-certified DREs currently in use as well.[30] The State also provided local registrars with cybersecurity training, such as detecting phishing attacks and how to protect passwords. Election officials worked closely with NPPD as well. Virginia has plans to begin conducting post-election audits; however, the audits will not begin until after the 2018 elections.

1 Associated Press. (2017, September 22) U.S. Tells 21 States That Hackers Targeted Their Voting Systems. Retrieved from https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html?mcubz=3

2 Larson, S. (2017, October 10). Hackers will work with government, academia to make future elections secure. Retrieved from http://money.cnn.com/2017/10/10/technology/defcon-hackers-voting-machine-coalition/index.html

3 NCSL. (2017, October 2). Online Voter Registration. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx

4 Reilly, K. (2016, August 30). Russians Hacked Arizona Voter Registration Database-Official. Retrieved from http://time.com/4472169/russian-hackers-arizona-voter-registration/

5 Fessler, P. (2017, September 22). 10 Months After Election Day, Feds Tell States More About Russian Hacking. Retrieved from http://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking

6 Congressional Research Service. (2016, October 18). The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election. Retrieved from https://fas.org/sgp/crs/misc/RS20898.pdf

7 NCSL. (2017, March 22). Electronic Poll Books, E-Poll Books. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

8 EAC. (2007, August). Compendium of State Poll Workers Requirements. Retrieved from https://www.eac.gov/documents/2010/05/14/compendium-of-state-poll-worker-requirements-poll-workers/

9 Ellis, E.G. (2016, November 8). Your Vote Counts. But How Does Your Ballot Get Counted? Retrieved from https://www.wired.com/2016/11/vote-counts-ballot-get-counted/

10 Verified Voting. (2016) The Verifier – Polling Place Equipment – November 2016. Retrieved from https://www.verifiedvoting.org/verifier/

11 Institute for Critical Infrastructure Technology. (2016, September). Hacking Elections is Easy! Part 1: Tactics, Techniques, and Procedures. Retrieved from http://icitech.org/icit-analysis-hacking-elections-is-easy-part-one-tactics-techniques-and-procedures/

12 Famighetti, C. & Norden, L. (2015, September 15). America's Voting Machines At Risk. Retrieved From https://www.brennancenter.org/publication/americas-voting-machines-risk

13 NCSL. (2016, June). Uniformity in Voting Systems: Looking at the Crazy Quilt of Election Technology. Retrieved from www.ncsl.org/Documents/Elections/The_Canvass_June_2016.pdf

14 Zarrelli, N. (2016, September 7). Election Fraud in the 1800s Involved Kidnapping and Forced Drinking. Retrieved from https://www.atlasobscura.com/articles/election-fraud-in-the-1800s-involved-kidnapping-and-forced-drinking

15 Mallonee, K. & Perez, E. (2016, September 27) DHS: 18 states seeking help securing elections. Retrieved from http://www.cnn.com/2016/09/27/politics/cybersecurity-rigged-election-homeland-security/index.html

16 Tin, A. (2016, October 28). Ahead of elections, states reject federal help to combat hackers. Retrieved from https://www.cbsnews.com/news/ahead-of-elections-states-reject-federal-help-to-combat-hackers/

17 Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Intelligence hearing titled "Russian Interference in the 2016 U.S. Elections." (2017, June 21). Retrieved from https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting

18 EAC. (2017, September 11) Voluntary Voting System Guidelines. Retrieved from https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

19 Lowry, B. (2016, August 30). Kansas partners with federal agencies to keep voter data secure. Retrieved from https://www.google.com/amp/amp.kansas.com/news/politics-government/election/article98851622.html

20 Hammill, R. (2016, April 26). Will Johnson County be ready for the 2016 presidential election. Retrieved from http://www.kansascity.com/news/local/community/joco-913/article74045762.html

21 Verified Voting. (2016) The Verifier – Polling Place Equipment –November 2016. Retrieved from https://www.verifiedvoting.org/verifier/#year/2016/state/20

22 Office of the Secretary of State. State of Kansas County Election Manual. Retrieved from https://www.kssos.org/forms/elections/County%20Election%20Manual%20(Combined).pdf

23 Eveld, E. (2016, January 25). Kris Kobach proposes voting-machine audits, files new voter fraud cases. Retrieved from https://www.google.com/amp/amp.kansascity.com/news/politics-government/article56474273.html

24 Torres, K. (2017, June 9). Judge dismisses paper-ballot lawsuit in Georgia's 6th District. Retrieved from http://www.ajc.com/news/state--regional-govt--politics/judge-dismisses-paper-ballot-lawsuit-georgia-6th-district/KDbQb7vQYL87fsnc3hPqoO/
25 Weise, E. (2017, August 24). Election hacking suit over Georgia race could be sign of what's to come. Retrieved from https://www.usatoday.com/story/tech/2017/08/24/election-hacking-lawsuit-over-heated-georgia-race-could-sign-whats-come/574313001/
26 New Jersey Office of Legislative Services. (2017, February 27) A4619. Retrieved from http://www.njleg.state.nj.us/bills/BillView.asp
27 The Ohio Legislature. (2017) Implement voting machine acquisition program. Retrieved from https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-135
28 Siegel, J. (2017, September 26). Bill offers Ohio counties 80 percent state funding for new voting machines. Retrieved from http://www.dispatch.com/news/20170926/bill-offers-ohio-counties-80-percent-state-funding-for-new-voting-machines
29 Fessler, P. (2017, September 26). Learning 2016's Lessons, Virginia Prepares Election Cyberdefenses. Retrieved September 27, 2017, from http://www.npr.org/2017/09/26/553519401/learning-2016-s-lessons-virginia-prepares-election-cyberdefenses
30 Virginia Department of Elections. (2017, September 8) Virginia Decertifies Paperless Voting Equipment. Retrieved from https://www.elections.virginia.gov/Files/Media/ELECTNewsRelease9-8-17.pdf

* Those states were Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Minnesota, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Texas, Virginia, Washington, and Wisconsin.

\+ Phishing is the attempt to obtain sensitive information such as usernames, passwords, or credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing is often carried out *via* email or instant messaging.

Δ This includes the four delegates to the House of Representatives from United States territories and the District of Colombia, and one Resident Commissioner from the Commonwealth of Puerto Rico.

± A form of electoral fraud in the United States during the 19th century by which unwilling participants were forced to vote, often several times over, for a particular candidate in an election.

For more information, please contact:

Katelin Neikirk, Research Analyst
Katelin.Neikirk@klrd.ks.gov

Joanna Dolan, Principal Research Analyst
Joanna.Dolan@klrd.ks.gov

Kansas Legislative Research Department
300 SW 10th Ave., Room 68-West, Statehouse
Topeka, KS 66612
Phone: (785) 296-3181
Fax: (785) 296-3824