KLRD

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

State and Local Government

I-4 Election Security

As further information has been released related to the scope of the attempted interference in the U.S. election process, election security has become an increasingly important policy topic at all levels of government. This article will examine the major election vulnerabilities and summarize election security activities being undertaken at the federal level as well as in Kansas and other selected states.

Recent reports, including the following examples, illustrate needed election security:

- In January 2017, the Office of the Director of National Intelligence released a declassified version of its report on interference in the 2016 election. The report states Russian intelligence obtained and maintained access to multiple U.S. state and local election boards. The Department of Homeland Security (DHS) stated the types of systems Russian actors targeted or compromised were not involved in vote tallying;
- In September 2017, DHS informed election officials in 21[1] states that hackers had targeted their voting system and sent more than 100 phishing e-mails to local election officials across the country before the 2016 election;
- In May 2018, hackers successfully shut down the Knox County, Tennessee, website and gained access to the server on that county's primary election day. The hackers shut down the website for an hour, but did not affect the outcome of the election;
- In July 2018, the U.S. Department of Justice (DOJ) announced indictments against 12 members of the Main Intelligence Directorate of the Russian General Staff (known as GRU). The indictment alleges that 11 members conspired to hack into computers and steal and release documents in an effort to interfere with the 2016 election, while 1 conspired to infiltrate computers of organizations responsible for administering elections; and
- In July 2018, the Federal Bureau of Investigation (FBI) informed Maryland officials that in 2015, without the State's knowledge, a Russian investor had purchased ByteGrid LLC, a software vendor that maintains part of the Maryland State Board of Elections' voter registration system.

Tools Used in Elections

There are many tools and resources used to increase the efficiency and security of elections. Since a majority of election tools are electronic, cybersecurity and tampering are major issues concerning election security. The tools and resources examined in this article include: online voter registration systems, electronic poll books, election personnel, voting devices, storage and tallying of ballots, transmission of vote tallies, and post-election audits.

Online voter registration systems. As with any online system, there are benefits and risks. Online voter registration can expedite new voter registration, updates to existing voter registrations, and finding other relevant information, such as locating polling places. However, online voter registration systems are at risk of a multitude of cyberattacks, as was seen when hackers targeted voting systems, including voter registration systems, in 21 states. While Arizona and Illinois were the only states with confirmed breaches of their voter registration systems, an NBC News article indicated five other states' voter registration systems were compromised with varying levels of severity. To date, no evidence has been found that any voter information was altered or deleted. However, the August 2018 Defcon conference (one of the world's largest hacking conventions), an 11-year-old was able to hack a replica of the Florida Secretary of State website and change election results in 10 minutes.

According to the United States Computer Emergency Readiness Team (US-CERT), potential cyberattacks on voter registration systems could include: phishing[2] attempts, injection flaws,[3] cross-site scripting vulnerabilities,[4] denial-of-service (DoS) attacks,[5] server vulnerabilities, and ransomware.[6]

US-CERT outlines several ways to protect voter registration systems, including patching applications and operating systems, application whitelisting,[7] restricting administrative privileges, input validation,[8] using firewalls, backing up voter registration data and storing it offline, conducting risk analysis, training staff on cybersecurity, having an incident response and business continuity plan in place and tested, and penetration testing.[9] The National Conference of State Legislatures (NCSL) also 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). As of March 2017, NCSL noted 30 states, including Kansas, permit the use of EPBs in some form. 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. EPBs are electronically connected to a central registration database. However, the Brennan Center for Justice (Brennan Center) 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. EPBs are vulnerable to many of the same risks as other computer tablets. The Center for Internet Security (CIS) identifies six major risks associated with EPBs: risks associated with established (whether persistent or intermittent) Internet connectivity; network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for EPBs; security weaknesses in the underlying commercial off-the-shelf product, whether hardware or software; security weaknesses in the dedicated components, whether hardware or software; errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media; and difficulties associated with finding and rolling back improper changes found after the fact.

The Election Assistance Commission (EAC) provides regulations created by Indiana, Ohio,

Pennsylvania, and Virginia. Based on regulations and guidance from these states, some ways in which EPBs can be secured include the use of secure sockets layer security,[10] use of a virtual private network,[11] and proper security training for staff.

Election personnel. One of the largest cybersecurity risks is human error. Potential security issues associated with election personnel include phishing e-mails; malware disguised as system patches; or the creation of unintentional gaps in cybersecurity, physical security, or both. One group of election personnel with a direct and important role on Election Day is poll workers. Poll workers are election officials, usually volunteers, responsible for ensuring proper and orderly voting at polling stations. Depending on the state, election officials may be identified as members of a political party or nonpartisan. Their duties can include issuing ballots to registered voters, registering voters, monitoring the voting equipment, explaining how to mark a ballot or use voting equipment, or counting votes.

An 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. 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. Most states, including Kansas, and many precincts do not require poll workers and other election personnel to be subject to background checks, which could allow "bad actors" unrestrained access to voting equipment and data.

Voting devices. In response to issues arising from the 2000 presidential election, Congress passed the 2002 Help America Vote Act (HAVA). The law provided almost $3.3 billion to help states replace voting systems and improve election administration. Voluntary technical standards for computer-based voting devices were first developed in the 1980s, but HAVA codified the development and required regular updating of voting device standards by the EAC. While the EAC guidelines are voluntary, most states, including Kansas, require their voting devices conform to EAC guidelines. On September 12, 2017, the EAC released a draft of new guidelines, which would require voting devices to produce a paper record that can be verified and audited. The new guidelines are expected to be approved in 2018. Below are descriptions of the two main types of voting devices in use today.

According to the Brennan Center, during the 2018 mid-term elections, 43 states and Washington D.C. were to use voting devices that are no longer manufactured; 13 states were to use paperless voting devices in some counties and towns; and 5 states were to use paperless voting devices statewide.

In July 2018, one of the top voting equipment manufacturers and software vendors, Election Systems & Software (ES&S), admitted to a Congressperson that ES&S installed remote-access software[12] on its voting devices between 2000 and 2006. In 2006, the source code for ES&S' remote-access software was stolen, which would allow hackers to examine the code and find vulnerabilities to exploit. Once discovered, ES&S informed customers; however, it was the customers' responsibility to remove the software. At least 60.0 percent of ballots cast in 2006 were tabulated on ES&S systems. However, ES&S announced in August 2018 it had formed new partnerships with multiple DHS offices to help conduct cyber-hygiene scans of ES&S public-facing Internet presence, monitor and share cyber-threat information, detect and report indicators of compromise, develop and distribute election security best practices, and raise election security awareness. ES&S also has installed ALBERT network security sensors[13] in its voter registration environments. The company has become a member of two Information Sharing and Analysis Centers (ISAC), including the Elections Infrastructure ISAC and the Information Technology ISAC, organizations that aim to improve cyber-threat information sharing between the private and public sectors.

Optical scan device. The most widely used device is the optical scan device, which is used in at least some polling places in every state. Voters

mark choices on paper ballots by hand or use an electronic ballot marking device and the ballots are read by an electronic counting device. Optical scan devices are regarded as more secure than direct recording electronic devices due to the fact the devices create a voter verifiable paper audit trail (VVPAT), meaning votes can be verified and cannot be altered electronically. However, as optical scan devices typically use electronic mechanisms 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 those choices are recorded directly to an electronic memory. Delaware, Georgia, Louisiana, New Jersey, and South Carolina all exclusively used DREs with no VVPAT in the 2016 election. However, all five states are currently either in the process of replacing their DREs or considering legislation to require such a change. DREs pose a unique concern because 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 DREs to produce a verifiable paper record of the voter's ballot. However, a voter must still review this ballot before casting it to verify it is correct. In November 2016, a former Central Intelligence Agency (CIA) Director noted DRE voting devices as a key vulnerability.

Limited life cycles. The average life span of electronic voting devices is less than ten years, and most of the devices currently in use have surpassed this age. Out-of-date devices and systems are not only more susceptible to technical issues, but also to cyberattacks and other means of tampering. The Institute for Critical Infrastructure Technology (ICIT) noted many voting devices have not been patched for almost a decade and use antiquated software that is unsupported by the manufacturer. The Brennan Center estimates the initial cost of replacing voting equipment throughout the United States could exceed $1.0 billion. However, many jurisdictions do not have the funds to replace outdated technology. Kansas statutes place financial and maintenance responsibilities for voting devices with the counties.

Storage of voting devices. ICIT found that many voting devices are stored in locations with minimal security, allowing election personnel relatively easy and unregulated access to alter or manipulate devices, either intentionally or unintentionally.

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 electronic tools. Security measures, such as passwords, specific access cards, encryption, and tamper-resistant tape, limit access to stored ballots. However, there are ways to circumvent these measures.

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. Paper ballots are tallied by hand or by a scanner that produces a printout 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 are tallied by hand; the other 95.0 percent are tallied either by voting devices or scanners. Voting devices and scanners can create issues, such as not calculating the votes correctly, not reading a ballot, or producing 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.

Transmission of vote tallies. After the votes have been tallied, the totals must be sent to a central location to determine the total vote tally of that race. Vote tallies are typically transmitted in one of the following ways: spoken over the phone to someone at election headquarters, who will input that data into a spreadsheet; some voting machines are equipped with modems that connect to a telephone line rather than the Internet, and can be transmitted electronically; or memory cards or sticks physically delivered

to voting headquarters, where it is turned over to election officials who will put the data storage device in their machines and download the actual results. Each of these methods has benefits and risks. Some of the risks could include "bad actors" providing altered or incorrect information; hackers infiltrating the systems used to transmit the tallies and altering or deleting the tallies; or simple human error.

Post-election audits. Currently, 32 states and the District of Columbia conduct some form of a post-election audit. NCSL has divided post-election audits into two categories:

- Traditional post-election audit: usually conducted manually by hand counting a portion of the paper records and comparing them to the electronic results produced by an electronic voting machine; and
- Risk-limiting audit: an audit protocol that makes use of statistical principles and methods and is designed to limit the risk of certifying an incorrect election outcome.

Twenty-nine states[14] and the District of Columbia require a traditional post-election audit, and Colorado, Rhode Island, and Virginia statutorily require risk-limiting audits. Kansas, North Dakota, and Wyoming conduct a repeat of the pre-election logic and accuracy test after the election to ensure voting machines are still tabulating accurately.

Other notable election security resources. States utilize a myriad of resources to protect their election infrastructure from outside attacks. These resources may include cyber-liability insurance,[15] white-hat hackers,[16] participation in interstate information sharing programs,[17] and cybersecurity services provided by private entities.[18]

Federal Government Current Activities

The 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 to state and local election officials and authorities from NCCIC, which helped stakeholders in federal departments and agencies, state and local governments, and the private sector manage their cybersecurity risks. 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. Eleven states, including Kansas, chose not to accept DHS' offer, citing concerns with federal intrusion on state elections.

On January 6, 2017, the Secretary of DHS determined that election infrastructure should be designated as a critical infrastructure sub-sector. Participation in the sub-sector is voluntary and does not grant federal regulatory authority. Elections continue to be governed by state and local officials, but with additional effort by the federal government to provide 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. As of March 2018, less than 12 states' election officials received their security clearance from DHS to receive information on election-related threats. Only 19 states have signed up for the risk assessments DHS is offering, and 14 are getting their "cyber-hygiene" scans. In July 2018, DHS announced the creation of the National Risk Management Center (Center), which will focus on evaluating threats and defending critical infrastructure against hacking. The Center will run simulations, tests, and cross-sector exercises to evaluate critical infrastructure weaknesses and threats.

In Fall 2017, the FBI established the Foreign Influence Task Force to identify and counteract the full range of foreign influence operations targeting U.S. democratic institutions. The Task Force works with personnel in all 56 FBI field offices and brings together the FBI's expertise in counterintelligence, cyber, criminal and counterterrorism, to root out and respond to foreign influence operations.

On February 20, 2018, the U.S. Attorney General ordered the creation of the DOJ Cyber-Digital Task Force, which will canvass the many ways the DOJ is combating the global cyber threat, and will also identify how federal law enforcement can more effectively accomplish its mission in this area. Among other areas, the Attorney General has asked the Task Force to prioritize its study of efforts to interfere with our elections. The Task Force released a report on July 19, 2018. The DOJ also issued a statement indicating the agency plans to alert American companies, private organizations, and individuals that they are being covertly attacked by foreign actors attempting to affect elections or the political process.

In early July 2018, the Director of the National Security Agency (NSA) directed the NSA and the Department of Defense's (DOD) Cyber Command to coordinate actions to counter potential Russian government-sanctioned interference in the 2018 midterm elections. The joint program is also working with the FBI, CIA, and DHS.

In August 2018, DHS, EAC, DOD, National Institute of Standards and Technology, NSA, Office of the Director of National Intelligence, U.S. Cyber Command, DOJ, the FBI, 44 states (including Kansas), the District of Columbia, and numerous counties participated in the Tabletop the Vote 2018, DHS' National Election Cyber Exercise which is a simulation that tested the ability of state and federal officials to work together to stop data breaches, disinformation, and other voting-related security issues.

EAC current activities. 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.

New HAVA funding. On March 23, 2018, the Consolidated Appropriations Act of 2018 (Act) was signed into law. The Act included $380.0 million in grants, which were made available to states to improve the administration of elections, including to enhance technology and make election security improvements. The majority of the funds will be used to improve election cybersecurity and to purchase new voting equipment.

Kansas Election Security Activities[19]

In February 2018, the Center for American Progress (CAP) released an analysis of election security in all 50 states. Kansas was ranked F/D, one of five states[20] that received an unsatisfactory ranking. The State received fair marks for voting machine certification requirements, pre-election logic and accuracy testing, and adherence to a number of minimum cybersecurity best practices. Kansas received unsatisfactory marks for the lack of a VVPAT from all voting devices and post-election audits; the State's ballot accounting and reconciliation procedures; and for allowing voters stationed or living overseas to return voted ballots electronically. [Note: At the time of the CAP report's publication, 2018 HB 2539 had not yet been passed.] Kansas received an incomplete mark for minimum cybersecurity for voter registration systems as CAP did not receive information on these topics from state officials.

Online voter registration system. Kansas is one of 37 states, and the District of Columbia, that offer online voter registration. The State's online voter registration system is about ten years old. The Kansas Director of Elections (Director) with the Office of the Secretary of State (Office) indicated in July of 2018 there was a firewall in place to protect the voter registration system, which was continuously updated, and that Office staff had been trained on cybersecurity best practices. The Secretary of State previously had stated in 2016 the voter registration system had logging capabilities to track modifications to the database.

Electronic poll books. As of April 2016, at least 16 Kansas counties, including Johnson, Sedgwick, Shawnee, and Wyandotte, were using EPBs, though neither state statutes nor rules and regulations provide guidance on their use, security, or maintenance. According to the Director, EPBs in Kansas are not connected to the voter registration system *via* a network. Counties are responsible for providing training on EPBs to election personnel.

Election personnel. Kansas poll workers must be residents of the area in which they will serve; normally at least 18 years of age, though they may be as young as 16 years old if they meet certain other requirements; not a candidate in the current election; and a registered voter in the area in which they will work. In Kansas, there are no requirements for poll workers to submit to and pass background checks. KSA 25-2806 requires county election officers to provide instruction concerning elections generally, voting devices, ballots, and duties for poll workers before each election. The curriculum specifics and training duration is left to the discretion of the county election officer.

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. As of March 2018, about 20 counties had replaced some or all of their voting devices or were in the process of purchasing new voting devices.

Johnson County (County) was one locality to update voting devices. In May 2018, the County contracted with ES&S for the purchase of 2,100 voting devices for $10.5 million. During the August 2018 primary election, there were issues obtaining data from the computer thumb drives where votes are stored. There were also issues with poll-worker preparedness in the event of device malfunction and insufficient paper ballots as a backup.

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. KSA 25-4406(k) requires voting devices to be compliant with HAVA voting system standards. Logic and accuracy testing must be conducted on all voting devices five days before an election, per KSA 25-4411. County commissioners and county election officers may select the type of voting device utilized in their voting locations, as long as it has been approved by the Secretary of State.

During the 2018 Legislative Session, the Legislature passed HB 2539, which required any electronic or electromechanical voting system purchased, leased, or rented by a board of county commissioners after the effective date of the bill to provide a paper record of each vote cast at the time the vote is cast. The bill also required voting systems to have the ability to be tested before an election and prior to the canvass date.

Storage and tallying of votes. The majority of Kansas counties use some form of paper ballot and use electronic scanners to tally the votes. These paper ballots are stored in locked boxes with authorized access. Counties that use DREs without a VVPAT store votes on removable memory cards.

Transmitting of vote tallies. Vote tallies provided *via* memory cards are transported by the county election officer. KAR 7-21-2 states results are only to be sent by fax, phone, handdelivery, or encrypted electronic transfer. According to the Office, officials typically call in or e-mail results, and there is no Internet uploading of results.

Post-election audits. During the 2018 Legislative Session, the Legislature passed HB 2539, which required county election officers to conduct a manual audit or tally of each vote cast in 1.0 percent of all precincts, with a minimum of one precinct located within the county. The audit requirements apply to all counties for elections occurring after January 1, 2019. The requirement for audit or tally applies regardless of the method of voting used. The bill specified these contested races will be audited:

- In presidential election years: one federal race, one state legislative race, and one county race;

- In even-numbered, non-presidential election years: one federal race, one statewide race, one state legislative race, and one county race; and
- In odd-numbered election years: two local races, selected randomly after the election.

Other election security resources. Kansas also uses participation in interstate information sharing programs and cybersecurity services provided by private entities to safeguard elections.

Kansas election funding. Kansas received $26.4 million in total 2002 HAVA funds and has $2.9 million remaining as of early 2018. Under the Consolidated Appropriations Act of 2018, Kansas received about $4.4 million in new HAVA funds, with a state match of $219,180. Kansas submitted a budget in August 2018 with the majority of funds going to local jurisdictions, purchase of new equipment, and training. The Office budget totals $4.5 million for FY 2018 and $4.6 million for FY 2019, all from special revenue funds. The Office budgeted $548,977 for elections and legislative matters for FY 2018 and $551,359 for FY 2019.

1 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.
2 Phishing includes forged e-mails, texts, and other messages used to manipulate users into clicking on malicious links or downloading malicious file attachments.
3 Injection flaw is a broad web application attack technique that attempts to send commands to a browser, database, or other system, allowing for a regular user to control behavior.
4 Cross-site scripting vulnerability allows threat actors to insert and execute unauthorized code in web applications
5 Denial-of-service attack prevents legitimate users from accessing information or services.
6 Ransomware is a type of malicious software that infects a computer system and restricts users' access to system resources or data until a ransom is paid to unlock it.
7 Application whitelisting allows only specified programs to run while blocking all others, including malicious software.
8 Input validation is a method of sanitizing untrusted user input provided by users of a web application.
9 Penetration testing is an authorized simulated attack on a computer system, performed to evaluate the security of the system.
10 Secure sockets layer security is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
11 Virtual private network creates a safe and encrypted connection over a less secure network.
12 Remote-access software allows someone to access a computer or a network from a remote distance.
13 ALBERT is a unique network monitoring solution that provides automated alerts on both traditional and advanced network threats, allowing organizations to respond quickly when their data may be at risk.
14 These states are Alaska, Arizona, California, Connecticut, Florida, Hawaii, Illinois, Iowa, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, and Wisconsin.
15 Cyber-liability insurance is coverage for financial consequences of electronic security incidents and data breaches.
16 White-hat hacker is a computer security specialist who breaks into protected systems and networks to test their security.
17 Interstate information sharing programs include the Multi-State Information Sharing & Analysis Center and the Election Infrastructure Information Sharing & Analysis Center, which collect, analyze, and disseminate threat information to members and provide tools to mitigate risks and enhance

resiliency.

18 Cybersecurity services provided by private entities include The Athenian Project and Project Shield.

19 *Note:* More detailed information on election security in Kansas can be found in the KLRD memorandum titled "Status of Election Security in Kansas," located at *http://www.kslegresearch.org/KLRD-web/Publications/StateLocalGovt/2018-08-08-ElectionSecurityKansas.pdf*.

20 The other states include Arkansas, Florida, Indiana, and Tennessee.

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