KLRD

Joanna Dolan
Principal Research Analyst
785-296-4440
Joanna.Dolan@klrd.ks.gov

Elections and Ethics

D-1 Election Security

Election security continues to be an important topic of discussion at all levels of government. This article examines the major election vulnerabilities and summarizes election security activities being undertaken at the federal level as well as in Kansas.

Tools Used in Elections

The Election Assistance Commission (EAC) noted more than 300,000 pieces of voting equipment were deployed during the 2018 election. Since a majority of election tools are electronic, cybersecurity and tampering are major issues concerning election security. Many tools and resources increase the efficiency and security of elections. The tools and resources examined in this article include online voter registration systems, electronic poll books, election personnel, voting machines, storage and tallying of ballots, transmission of vote tallies, post-election audits, and other cybersecurity tools.

Online voter registration systems. The EAC found there were more than 211 million registered voters during the 2018 election. According to the National Conference of State Legislatures (NCSL), currently 37 states and the District of Columbia (D.C.) use an online voter registration system to register those voters.

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 election information, such as locating polling places. However, online voter registration systems are at risk of cyberattacks, as was seen when hackers targeted election systems, including voter registration systems, in 21 states. While Arizona, Florida, and Illinois were confirmed to have breaches of their voter registration systems, an NBC News article[1] indicated four other states' voter registration systems were compromised to varying levels of severity. To date, no evidence has been found that any voter information was altered or deleted.

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

were made inaccessible or changed during the voting period, the interference could result in long lines and confusion, leading some voters to become discouraged and potentially not vote.

US-CERT outlines several ways to protect voter registration systems, including patching applications and operating systems, application whitelisting,[6] restricting administrative privileges, input validation,[7] 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 tested and in place, and penetration testing.[8] NCSL also cites several approaches to ensure voter registration security, including requiring registrants to provide 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 all jurisdictions transition to electronic poll books (EPBs). The EAC indicates that 36 states and D.C. used EPBs during the 2018 election, with seven of these states using EPBs in all election jurisdictions. 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 either *via* the Internet or a closed network. This connection could be either at the time of downloading the list onto the device or during the entire time the device is in use. However, the Brennan Center for Justice (Brennan Center) notes there are no accepted technical standards for these connections 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 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,[9] use of a virtual private network,[10] 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 in election security 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.

During the 2018 election, there were more than 600,000 poll workers nationwide, with more than two-thirds of those being older than 61 years of age. The most recent EAC 50-state survey of requirements for poll workers notes that in all states and territories, poll workers must generally be at least 18 years old; be registered to vote in that state; and be a resident of the county or

district in which they will work. A majority of states, including Kansas, require poll workers to receive training, but the type, frequency, intensity, and requirements for who is trained vary greatly. Most states, including Kansas, and many precincts do not require poll workers and other election personnel to be subject to background checks, which pose potential risks concerning who has access to voting equipment and data.

Voting machines. In response to issues identified during 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 machines were first developed in the 1980s, but HAVA instituted the development and required regular updating of voting machine standards by the EAC. While the EAC guidelines are voluntary, most states, including Kansas, require their voting machines conform to EAC guidelines. The EAC adopted the Voluntary Voting Systems Guidelines (VVSG) Version 2.0 in September 2017.

According to NSCL, nine states[11] and D.C. require election machine testing to federal standards, including standards set by the Federal Election Commission (FEC), National Institute of Standards and Technology (NIST), and the EAC; 17 states[12] require testing by a federally accredited lab; 12 states[13] require full federal certification; and 4 states[14] refer to federal agencies or standards, but do not fall into any of the previous categories.[15]

More than 330,000 pieces of voting equipment to cast and tabulate votes were deployed for the 2018 election. The EAC indicated almost 90.0 percent of election jurisdictions used voting machines equipped with some form of paper backup, and less than 2.0 percent of jurisdictions relied solely on voting machines with no paper backup. As of August 2018, 38 states require some element of federal testing and certification of election systems before installing them in their state. Eight states do not require such testing or certification.

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[16] 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[17] in its voter registration environments. The company has become a member of two Information Sharing and Analysis Centers (ISACs), 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.

The EAC notes ballot-marking devices (BMDs) were the most widely used type of voting equipment in 2018. Following are descriptions of the two main types of voting equipment used to count votes.

Optical scan device. Optical scan devices were used in almost 80.0 percent of election jurisdictions. The optical scan device is used in at least some polling places in every state. Voters mark choices on paper ballots by hand or use an electronic BMD, and the ballots are read by an electronic counting device. Optical scan devices are regarded as more secure than direct recording electronic devices because they create a voter verifiable paper audit trail (VVPAT), meaning votes can be verified and cannot be altered electronically. However, as optical scan devices use electronic mechanisms to count ballots, vote counts are vulnerable to cyberattacks, though an

audit of the paper ballots is likely to catch any irregularities.

Direct recording electronic machine. The direct recording electronic voting machine (DRE) allows voters to mark choices *via* a computer interface and those choices are recorded directly to an electronic memory. Delaware, Georgia, Indiana, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, and Tennessee all used DREs with no VVPAT in at least half their election jurisdictions during the 2018 election. 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 machine'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 machines as a key vulnerability.

Limited life cycles. The average life span of electronic voting machines is less than ten years, and most of the machines in use are out of date and unable to be updated. 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. Many jurisdictions do not have the funds to replace outdated technology. Kansas statutes place financial and maintenance responsibilities for voting devices with the counties. Based on the narratives provided by the states receiving federal election grant funding, 34 states[18] and D.C. are in the process of updating or replacing their voting equipment. New Mexico and Rhode Island replaced voting equipment statewide in 2014 and 2016, respectively.

Outdated voting machines and software can also result in issues such as vote-flipping, where a voter selects one candidate but the machine records another candidate. In October 2018, the Texas Director of Elections issued an election advisory stating certain voting machines, specifically the Hart eSlate system, were changing one or more voter selections from one candidate to another when voters simultaneously turned a selection dial and hit the "enter" button. Eighty-two of the 254 counties in Texas have these machines. The issue with the eSlate machine first surfaced in the 2016 presidential election. Voters in Georgia, Nevada, North Carolina, Pennsylvania, and Tennessee also reported vote-flipping during the 2016 presidential election.

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

Storage and tallying of ballots. The EAC indicates the vast majority of ballots cast in person on Election Day are counted at the precinct or polling location. Provisional ballots are typically counted either partially or entirely at a central location.

While paper ballots are stored in physical ballot boxes, electronic ballots are stored on machine smart cards, a machine's random-access memory, or other electronic devices. Security measures, such as passwords, specific access cards, encryption, and tamper-resistant tape, limit access to stored ballots. However, these measures are not foolproof.

Election results are also vulnerable 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 5.0 percent of ballots in the United States are tallied by hand, while the other 95.0 percent are tallied either by voting devices or scanners. Voting devices and scanners can experience errors, 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 deliberate error, as it would be difficult to intentionally alter, switch, or destroy ballots without being detected. However, there is still the possibility of human error.

Transmission of vote tallies. After 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 they are turned over to election officials who put the data storage device in their machines and download the actual results. Some voting machines allow preliminary results to be transferred to a county office using the same kind of modem found in smart phones, rather than being physically carried from each polling station. While this method of transmission allows early results to be shared instantly, it also means the data is only as secure as the cellular company carrying it. Such connections, which not only transmit data but also receive it, provide yet another potential system weakness.

Each of these methods has risks. Some of the risks 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.

A secure means of communicating preliminary or final vote counts to the media and public are also important. Some election officials may choose to utilize official election websites or social media accounts to communicate this information. If a bad actor was able to manipulate the website or account to display incorrect information or take down the website or account all together, this could lead to confusion and frustration, as well as damaging public trust in election officials.

Post-election audits. Currently, 37 states and D.C. require 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.

Thirty-two states[19] and D.C. require a traditional post-election audit, and Colorado, Nevada, Rhode Island, and Virginia statutorily require risk-limiting audits.

See *D-4 Post-election Audits* in this *Briefing Book* for more information.

Internet Voting

The EAC reported Uniform and Overseas Citizens Absentee Voting Act (UOCAVA) voters are increasingly using electronic means to receive and return absentee ballots. E-mail was the most popular electronic transmission method, with 56.6 percent of UOCAVA voters receiving their absentee ballots and 29.6 percent returning the ballot *via* e-mail. Voting securely through the Internet places much of the security responsibility on the voter and the security measures they have in place on their devices. Although it is possible to strengthen a wireless connection against an attacker for such applications, doing so is not easy and can be easily misconfigured. Also, these stronger protections can be difficult to use and maintain, especially for those unfamiliar with the technology.

In 2018, West Virginia began using a block chain-enabled[20] mobile voting application, called Voatz, for overseas residents from 24 counties. Approximately 140 voters from 31 counties voted in 2018 using the application. Voters must submit a selfie and photo identification as well as go through a multi-factor authentication process to log in. However, the security of a vote would still depend greatly on the security of the device on which the vote was made.

Other notable election security resources. States utilize a myriad of resources to protect their election infrastructure from outside attacks. These resources may include enlisting the help of the National Guard, cyber-liability insurance,[21] white-hat hackers,[22] participation in interstate information sharing programs,[23] and cybersecurity services provided by either the federal government or private entities.[24]

Current Federal Government 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 membership 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. In a Senate hearing, then-Secretary of Homeland Security stated 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 Homeland Security determined 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. According to a report from the Office of the Inspector General, as of July 2018, 87 of the 100 eligible states' election officials received their interim or full security clearance from DHS to receive information on election-related threats. Fully granted clearances were provided to 43 officials and 44 were granted on an interim status. Only 19 states have signed up for the risk assessments DHS is offering, and 14 are conducting "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 to canvass the ways the DOJ addresses the global cyber threat. The Task Force 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 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 July 2018, DHS announced the creation of the National Risk Management Center (NRMC) within the Cybersecurity and Infrastructure Agency. The NRMC is a centralized location for government and private sector partners to share information related to digital security.

In August 2018, DHS, EAC, DOD, NIST, NSA, Office of the Director of National Intelligence, U.S. Cyber Command, DOJ, the FBI, 44 states (including Kansas), D.C., 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.

Executive Order (EO) 13848 was issued in September 2018, declaring a national emergency regarding foreign influence and interference with election processes and equipment. The EO allows the imposition of sanctions on any person, entity, or foreign government who is found to be attempting or has interfered with U.S. election processes or equipment.

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. The EAC has also added a page to their website concerning election security preparedness, with many links to valuable information on how to secure election systems, guides on what to do during and after a cyber incident, and glossaries for commonly used terms (*https://www.eac.gov/election-officials/election-security-preparedness/*).

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 is for election cybersecurity and to purchase new voting equipment.

Kansas Election Security Activities

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[25] 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. See more information on HB 2539 under sections "Voting Devices" and "Post-election Audits" in this article.] Kansas received an incomplete mark for minimum cybersecurity for voter registration systems due to the absence of information from state officials on these topics.

Online voter registration system. Kansas is one of 37 states, and D.C., 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 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 a resident and registered voter in 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; and not a candidate in the current election. 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. According to the EAC, Kansas deployed a total of 6,365 voting machines for the 2018 elections; 894 DREs without VVPAT, 57 DREs with VVPAT, 4,461 BMDs, and 953 electronic scanners. 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 of the localities that updated its 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.

Kansas 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, pursuant to 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 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 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, hand delivery, 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 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 federal election funding. Kansas submitted a budget in August 2019, with the majority of funds going to local jurisdictions, purchase of new equipment, and training, which has not yet been approved by the Governor or the Legislature. The Office budget totals $6.1 million for FY 2020 and $5.4 million for FY 2021, all from special revenue funds. The Office budgeted $710,893 for elections and legislative matters for FY 2020 and $492,977 for FY 2021.

Kansas received $26.4 million in total 2002 HAVA funds. Under the Consolidated Appropriations Act of 2018, Kansas received about $4.4 million in new HAVA funds, with a state match of $219,180. If the revised budget request is approved, the Office would retain approximately $3.0 million in federal funds between the 2002 HAVA Title I funds and the 2018 HAVA funds at the end of FY 2021.

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

1 Arkin, W.; Dilanian, K.; McFadden, C. *U.S. Intel: Russia compromised seven states prior to 2016 election*. (2018, February 27). Retrieved from https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296.
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 An 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 Application whitelisting allows only specified programs to run while blocking all others, including malicious software.
7 Input validation is a method of sanitizing untrusted user input provided by users of a web application.
8 Penetration testing is an authorized simulated attack on a computer system, performed to evaluate the security of the system.
9 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.
10 A virtual private network creates a safe and encrypted connection over a less secure network.
11 Connecticut, Hawaii, Indiana, Kentucky, Nevada, New York, Tennessee, Texas, and Virginia.
12 Alabama, Arkansas, Arizona, Colorado, Illinois, Iowa, Massachusetts, Maryland, Michigan, Minnesota, Missouri, New Mexico, Oregon, Pennsylvania, Rhode Island, Utah, and Wisconsin.
13 Delaware, Georgia, Idaho, Louisiana, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Washington, West Virginia, and Wyoming.
14 Alaska (the director may consider whether the FEC has certified a voting machine); California (the Secretary of State adopts testing standards that meet or exceed the federal voluntary standards set by the EAC); Kansas (requires compliance with HAVA voting system standards); and Mississippi (DREs shall comply with the error rate standards established by the FEC; *Note:* the FEC no longer sets voting system standards).
15 NCSL. *Voting System Standards, Testing and Certification.* (2018, August 8). Retrieved from http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

16 Remote-access software allows someone to access a computer or a network from a remote distance.

17 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.

18 Alabama, Alaska, Arkansas, California, Connecticut, Delaware, Georgia, Hawaii, Idaho, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Utah, Vermont, West Virginia, and Wyoming.

19 Alaska, Arizona, California, Connecticut, Florida, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, and Wisconsin.

20 A blockchain is resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

21 Cyber-liability insurance is coverage for financial consequences of electronic security incidents and data breaches.

22 A white-hat hacker is a computer security specialist who breaks into protected systems and networks to test their security.

23 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.

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

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

For more information, please contact:

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

Jessa Farmer, Research Analyst
Jessa.Farmer@klrd.ks.gov

Jill Shelley, Principal Research Analyst
Jill.Shelley@klrd.ks.gov

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