KANSAS LEGISLATIVE RESEARCH DEPARTMENT

68-West–Statehouse, 300 SW 10th Ave.
Topeka, Kansas 66612-1504
(785) 296-3181 ◆ FAX (785) 296-3824
kslegres@klrd.ks.gov http://www.kslegislature.org/klrd

August 8, 2018

STATUS OF ELECTION SECURITY IN KANSAS

As further information has been released related to the scope of the attempts to interfere in the United States' election process, election security has become an increasingly important policy topic at all levels of government. This memorandum will provide an overview of the current status of election security in Kansas. Topics to be addressed include: an overview of election equipment, the associated risks, and expert guidance on how to mitigate those risks; an overview of the current security status of Kansas' election equipment and processes; Kansas' work with the U.S. Department of Homeland Security (DHS); funding of election security in Kansas; and an overview of Colorado's election systems.

A glossary of terms is located at the end of this memorandum for ease of reference.

Election Tools and Resources

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 memorandum include online voter registration systems, electronic poll books, election personnel, voting devices, storage and tallying of ballots, transmission of vote tallies, post-election audits, and other election security resources.

Online Voter Registration Systems

As with any online system, there are benefits and risks. Online voter registration can: expedite new voter registration; make updates to existing voter registrations; and help locate other relevant information, such as locating your polling place. However, online voter registration systems are at risk of a multitude of cyberattacks. This was demonstrated during the 2016 presidential election, when hackers targeted voting systems, including voter registration systems, in 21* states.[1] While Arizona and Illinois were the only states with confirmed breaches of their voter registration systems, news reports indicated five other states' voter registration systems have been compromised with varying levels of severity. To date, no evidence has been found that any voter information was altered or deleted.[2]

According to the United States Computer Emergency Readiness Team (US-CERT), potential cyberattacks on voter registration systems could include: phishing attempts, injection

**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.*

flaws, cross-site scripting (XSS) vulnerabilities, denial-of-service (DoS) attacks, server vulnerabilities, and ransomware.[3]

US-CERT outlines several ways to protect voter registration systems, including: patching applications and operating systems, application whitelisting, restricting administrative privileges, input validation, 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.

The National Conference of State Legislatures (NCSL) also cited several approaches used to ensure 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 each question on a different screen.

Electronic Poll Books

In January 2014, the Presidential Commission on Election Administration recommended jurisdictions transition to electronic poll books (EPBs).[4] 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.

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:[5]

- 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 Congressional Research Service notes there are no accepted technical standards for EPBs and there are concerns about security and fraud prevention, especially for those

connected to remote computers *via* the Internet. However, several states have established rules and regulations or guidelines for EPB usage. The Election Assistance Commission (EAC) provides this information for Indiana, Ohio, Pennsylvania, and Virginia.[6] Based on regulations and guidance from these states, some ways in which EPBs can be secured include the use of secure sockets layer security or the use of a virtual private network, and proper security training for staff who will be using EPBs.

Election Personnel

According to a report by Shred-it, an information security company, 47.0 percent of business leaders said human error, such as accidental loss of a device or document by an employee, had caused a data breach at their organization. Among employees, over 25.0 percent said they leave their computer unlocked and unattended.[7] While this report was focused on businesses, it provides incite into one of the largest cybersecurity risks – 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 that play a direct and important role on election day are 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 non-partisan. 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.[8] Most states and precincts do not require poll workers and other election personnel be subject to background checks, which could allow "bad actors" unrestrained access to voting equipment and data. Election personnel, especially poll workers, need to receive training on cybersecurity best practices and should undergo background checks to prevent any "bad actors" from gaining access to election equipment.

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.[9] The new guidelines are expected to be approved in 2018. Below are descriptions of the two main types of voting devices in use today.

Optical scan device. 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 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 that 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 (DRE) device, 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 paper trail in the 2016 election.[10] 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 DRE devices to produce a verifiable paper record of the voter's ballot. However, a voter must review this ballot before casting it for this concern to be alleviated.

Other concerns with voting devices include:

Limited life cycle. 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.[11] The Brennan Center estimates the initial cost of replacing voting equipment throughout the United States could exceed $1.0 billion.[12] Many jurisdictions do not have the funds needed to replace outdated technology.

Storage of Voting Devices. It is also important to consider how voting devices are stored and who may have access to them. According to ICIT, 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. This poses a critical risk to the security and reliability of voting devices.

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 the stored ballots. However, there are ways to circumvent these measures, for example 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. 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 were tallied by hand; the other 95.0 percent are tallied either by the voting device or scanners.[13] 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.

Transmitting Vote Tallies

After the votes have been tallied in precincts, the precinct totals must be sent to a central location to determine the state or district-wide total vote tally for that race. Vote tallies typically are transmitted in one of the following ways:[14]

- Spoken over the phone to someone at election headquarters, who inputs that data into a spreadsheet;
- Electronically *via* modems connected to a telephone line, not the Internet; or
- Memory cards or sticks physically delivered to voting headquarters, where they are turned over to election officials, who download the actual results from the data storage devices onto their own machines.

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 Colombia conduct some form of a post-election audit. NCSL has divided post-election audits into two categories:[15]

- *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. Some states have a process by which some or all of the audit can be conducted electronically. This may be done with the assistance of a computer or a tabulation device other than the one initially used to tabulate results. Some traditional post-election audits use a "tiered" system, which means a different number of ballots are reviewed, depending on the margin of victory; 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. If the margin is larger, fewer ballots need to be counted. If the race is tighter, more ballots are audited.

Twenty-nine states[^] and the District of Colombia require a traditional post-election audit; Colorado, Rhode Island, and Virginia statutorily require risk-limiting audits; and Ohio and Washington provide options for counties to run different types of audits, including risk-limiting

^Alaska, Arizona, California, Connecticut, District of Columbia, Florida, Hawaii, Illinois, Iowa, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Jersey (although the state currently does not have machines that produce a paper record and therefore cannot yet meet this requirement), New Mexico, New York, North Carolina, Ohio (though risk-limiting audits are recommended but not required), Oregon, Pennsylvania, Tennessee, Texas, Utah, Vermont, Washington (counties have the option of conducting a risk-limiting audit), West Virginia, and Wisconsin.

audits. Many experts have labeled risk-limiting audits as the gold standard, and the American Statistical Association also endorsed this type of post-election audit in 2010.[16]

Kansas, North Dakota, and Wyoming conduct a repeat of the pre-election logic and accuracy test after the election to ensure that voting machines are still tabulating accurately. Before an election, election officials create a "test deck" of ballots that are run through tabulators to ensure races are being accurately recorded and tabulated. In these states, the same test deck is run through the machines after the election, to once again test the accuracy of the machines.[17]

Other Election Security Resources

Cyber Liability Insurance. In 2015, there were 63 reported breaches of government and military databases, with over 34.2 million records compromised, according to the National Association of State Procurement Officials (NASPO). A NASPO research brief indicated the average cost of a data breach in 2016 was $4.0 million, or $158 per record. Large scale distributed denial of service (DDoS) attacks can be bought for just $20 online, but can create millions of dollars of damage a state must manage.[18]

Cyber liability insurance, also known as cyber risk insurance or cyber breach insurance, is coverage for the financial consequences of electronic security incidents and data breaches. Some states choose to obtain cyber liability insurance for their own networks, some require vendors to obtain certain types of coverage, and others use a mixture of both methods. The most common coverage components include: data breach and privacy risk management; breach response coverage; business interruption coverage; fiduciary liability coverage; cyber extortion/ransomware coverage; media liability coverage; and professional liability coverage. In March 2018, Verisk Analytics, Inc.'s VRSK business, ISO, announced that 42 states and U.S. territories have implemented its cyber insurance program.[19]

In 2014, Montana experienced a data breach of up to 1.3 million public health records containing sensitive information. The State had a $2.0 million cyber liability insurance policy that covered costs associated with setting up a toll-free help line, free credit monitoring for those exposed, and the mailing of notification letters. Without the coverage Montana would have had to shoulder all these costs as well as the costs of restoring its systems and additional security upgrades.[20]

Information on other states with cyber liability insurance and the associated costs is included in the following table.[21]

State	Purchase Date	Yearly Cost	Coverage	Deductible
Georgia	2017	$1,800,000	$100,000,000	$250,000
Montana	2011	$88,200	$2,000,000	$100,000 and 10.0 percent co-payment for credit monitoring
Utah	2015	$230,000	$10,000,000	$1,000,000

White-hat hackers. Some states are turning to white-hat hackers (white-hats) to uncover vulnerabilities in computer networks. A few have even begun considering "bug bounties," which is when a company or other entity offers individuals recognition and/or compensation for reporting bugs. White-hats simulate threats, set up phishing scenarios, and may even attempt in-office hacks. According to a 2016 study by the National Association of State Chief Information Officers and Deloitte & Touche LLP, nearly half of state information

technology officials reported they sometimes used third-parties to attempt to penetrate their systems. One-third of those officials said they did so at least once a year.[22] For example, Delaware regularly hires white-hat hackers to conduct penetration testing at a cost of $10,000 to $25,000. Missouri also hires white-hat companies for penetration testing, which lasts several weeks and costs about $90,000. The State is also looking into conducting bug bounties.

Interstate Information Sharing. CIS is responsible for the operation of the Multi-State Information Sharing & Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing & Analysis Center (EI-ISAC), both of which collect, analyze, and disseminate actionable threat information to their members and provide tools to mitigate risks and enhance resiliency.[23] The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for state, local, territorial, and tribal (SLTT) governments. Membership is free and open to all SLTT governments. MS-ISAC members currently include representatives from all 50 states, hundreds of local governments, and several tribal and territorial governments. The MS-ISAC Computer Emergency Response Team (MS-ISAC CERT) can provide malware analysis, reverse engineering, log analysis, forensics analysis, and vulnerability assessments. The Incident Response service is available to all SLTT entities, even without MS-ISAC membership.[24] The EI-ISAC, which was launched in March 2018, provides election agencies with access to an elections-focused cyber defense suite, which includes sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices. Membership is free and open to all SLTT governments.[25] Currently, 830 counties and all 50 states have joined.[26]

Albert. CIS, *via* the MS-ISAC offers network security monitoring services through a solution referred to as Albert.[27] Albert grew out of a DHS Einstein project, which focused on detecting and blocking cyberattacks within federal agencies. DHS approached CIS about creating a similar capability for states and localities. This service is available to U.S. SLTT government entities. If something is picked up by Albert, an alert is sent to the Security Operations Center at the MS-ISAC where it is reviewed in-person. If the threat is legitimate, the state or locality where it was detected is contacted. According to CIS Vice President of Operations, Brian Calkin, Albert is already deployed in all 50 states, but not necessarily for election infrastructure.[28] An early CIS analysis shows about half of the states have election systems connected to Albert. The other half were expected to be connected by late spring or early summer 2018.

The Athenian Project. Cloudflare, a company that provides free cybersecurity services to at-risk public interest websites that may be subject to cyberattack, recently launched the Athenian Project (Project).[29] The Project is designed to protect state and local government websites tied to elections and voter data from cyberattack and keep them online. Specific services offered include: DDoS protection; web application firewall (WAF) with pre-built and custom rule sets; rate limiting; professional implementation; “under attack” emergency support engineer; and 24/7/365 phone, email, and chat support. State and local governments may receive free services if their website is owned and managed by a state, county, or municipal government, and the website is related to the administration of elections, voter data, or the reporting of election results. Former EAC Commissioner, Matthew Masterson, recommended the Project as a potential resource for election officials.[30] The State of Alabama also utilized the Project to protect its website during the December 2017 special general election for the U.S. Senate.[31]

Project Shield. Project Shield (Shield) is a free anti-DDoS service that is offered by Jigsaw, a subsidiary of Google’s parent company, Alphabet Inc. Shield acts as a reverse proxy

to filter harmful traffic and absorb traffic through caching. Shield accepts applications from news; human rights and elections monitoring organizations; individual journalists; all federal, state, and local candidates, political parties, political committees, and Section 527 organizations. Shield currently safeguards about 700 websites from DDoS attacks.[32]

Kansas Election Security Activities

In February 2018, the Center for American Progress (CAP) released an analysis of election security in all 50 states.[33] The publication ranked states on a scale from A, which is good, to F, which is unsatisfactory. No state received an A. Kansas was ranked F/D, one of 5 states that received an unsatisfactory ranking.** Among Kansas' neighboring states, Iowa, Nebraska, and Oklahoma all received C rankings; Missouri received a D; and Colorado received a B ranking. 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, HB 2539 had not yet been passed.]* The State received fair marks for voting machine certification requirements and pre-election logic and accuracy testing. Kansas received an incomplete mark for minimum cybersecurity for voter registration systems as CAP did not receive information on these topics from state officials.

CAP did note that Kansas does adhere to a number of minimum cybersecurity best practices. For example, in 2004, the Office of the Secretary of State (SOS) implemented a voting system security policy stating:

- Voting systems 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 with limited, authorized access.[34]

Online Voter Registration Systems

Kansas is one of 37 states, and the District of Colombia, who offer online voter registration.[35] The State's online voter registration system is about ten years old. The SOS, Office of Information Technology Services (OITS), and a private vendor are responsible for the maintenance and security of the voter registration system. The Kansas Director of Elections (Director) with the SOS, indicated there is a firewall in place to protect the voter registration system, which is continuously updated. He also stated the voter registration system is backed up and a risk analysis has been conducted, but did not state the frequency or how recently these activities were conducted. According to the Director, Kansas utilizes the same software vendor as Arizona for the state's voter registration database. However, Kansas has at least one

** The other states included: Arkansas, Florida, Indiana, and Tennessee.

significant additional layer of security above the Arizona system, which was breached during the 2016 Presidential Election.[36] According to a 2014 policy memorandum from OITS, the voter registration system provides access control to ensure that only authorized personnel have access.[37] The same policy memorandum indicates the State also performs regular vulnerability assessments and penetration testing and has an intrusion detection system. The current SOS stated the voter registration system has logging capabilities to track modifications to the database.[38] The Director also indicated SOS staff has been trained on cybersecurity best practices, but did not specify the type of training or the frequency. Further information provided by the Director stated the SOS has an incident response and continuity plan in place. Information on when it was established and last reviewed and tested was not provided.

Electronic Poll Books

As of March 2017, NCSL noted 30 states, including Kansas, permit the use of EPBs in some form.[39] 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.[40] According to the Director, EPBs in Kansas are not connected to the voter registration system *via* a network. He did not provide information on how data from the voter registration system is accessed by EPBs. As indicated by the Director, counties are responsible for providing training on EPBs to election personnel.

Election Personnel

There are several different individuals involved in the administration of elections in Kansas. This section will focus on poll workers because they have the most direct interaction with voters and their ballots. In Kansas there are two types of poll workers, clerks and supervising judges. Applicants for both roles must meet the same requirements. Kansas 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; not a candidate in the current election; and a registered voter in the area in which they will work.[41] In Kansas and many other states, there are no requirements for poll workers to submit to and pass background checks or participate in other extensive vetting procedures. The SOS does check individuals listed as election board workers against the current Kansas Bureau of Investigation list of sexual predators before every election. No poll workers have unsupervised access to voting or tallying devices or ballots.

A majority of states, including Kansas, require poll workers to have some training, but the type, frequency, intensity, and persons required to be trained, varies greatly. 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. Depending on the size of the county and the resources available, the training can vary greatly between counties.

Voting Devices

In the 2016 Presidential election, data from Verified Voting showed that 70 Kansas counties used paper ballots, 15 used both paper ballots and DREs without VVPAT, 15 used DREs without VVPAT, and 5 used DREs with VVPAT. In January 2016, the Kansas SOS also encouraged the use of voting devices that produce a paper trail.[42] To date, the SOS has not requested funding from the Kansas Legislature to replace devices that do not produce 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, according to information obtained by the Kansas Legislative Research Department (KLRD).

Statutes concerning electronic voting devices can be found in The Electronic and Electromechanical Voting Systems Act (KSA 25-4401 through KSA 25-4416), and statutes concerning optical scan voting devices can be found in The Optical Scanning Voting Systems Act (KSA 25-4601 through 25-4615). Kansas requires voting devices to be compliant with HAVA voting system standards and other federal statutes and regulations governing voting equipment.[43] County commissioners and the county election officers are responsible for the purchase, maintenance, and storage of voting devices and equipment, and may select the type of voting device utilized in their voting locations, as long as it has been approved by the SOS.[44] Pursuant to KSA 25-4411, Kansas requires that logic and accuracy testing be conducted on all voting devices five days before an election.

During the 2018 Legislative Session, the Legislature passed HB 2539, which contained the contents of HB 2333. The bill 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 the voting systems to have the ability to be tested both before an election and prior to the canvass date. The ability to match the paper record of the machine to the vote total contained in the machine is part of the required testing. The bill did not amend additional requirements in continuing law for electronic or electromechanical voting systems.

Storage and Tallying of Votes

The majority of Kansas counties use some form of paper ballot, either one marked and printed by an optical scan voting device or a pre-printed paper ballot that is marked by hand, and use electronic scanners to tally the votes, according to information provided to KLRD in March 2018. These paper ballots are stored in locked boxes with authorized access.

Counties that use DREs without a VVPAT store votes on removable memory cards. The SOS advises counties that memory cards in each touch screen voting station should be stored within a locked compartment.[45] The supervising judge should be the only person with a key to this compartment. The memory cards or ballots from each voting location are transported from the voting location to the county elections office by a sworn election official or a sworn law enforcement officer. Voting machines and ballot boxes should be sealed before delivery to polling place locations. Seals should be tamperproof and serialized with numbers. Logging of machine serial number, seal number, and designated voting location is an essential part of the audit trail.

Transmitting of Vote Tallies

Vote tallies provided *via* memory cards are transported by the county election officer, who is also responsible for keeping track of all memory cards, whether in transit or in the polling location. In the SOS 2004 Voting Security Policy, the SOS states results from elections should not be sent from polling places to election offices *via* modem, network, phone line, cable, or any other electronic form of file transmission. The same applies when sending results from the county election office to the SOS. KAR 7-21-2 states results are only to be sent by fax, phone, hand-delivery, or encrypted electronic transfer. The current SOS has said officials typically call in or email results and there is no internet uploading of results.[46]

Post-Election Audits

In January 2016, the SOS 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.[47]

During the 2018 Legislative Session, the Legislature passed HB 2539, which contained the contents of HB 2333.[48] The bill 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 precinct(s) audited will be selected randomly after the election. The SOS is required to adopt rules and regulations governing the conduct and procedure of election audits, including the random selection of precincts and offices involved in audits. 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.

The SOS is still in the process of developing the rules and regulations necessary to implement these audits.

Other Resources

Cyber Liability Insurance. The Kansas Interim Chief Information Security Officer (CISO) stated that, to his knowledge, cyber liability insurance is not used by any Kansas state agency.

White-hat hackers. The Interim CISO indicated that while Kansas does not currently use white-hat hackers, the State has been using penetration testing, which provides a similar function, for many years. He was unable to confirm if the SOS uses penetration testing for their systems.

Interstate Information Sharing. A representative of CIS stated Kansas has been a member of MS-ISAC since June 2012 and joined EI-ISAC in April 2018. Seventeen counties and the SOS are members of EI-ISAC.[49]

Albert. According to CIS, the SOS utilizes Albert. However, CIS could not provide information concerning how long the SOS has utilized Albert.

The Athenian Project. According to a Project representative, no Kansas entities are currently working with the Project.

Project Shield. KLRD was unable to obtain information on whether the SOS works with Shield.

Notable Recent State Legislation

SB 56.[50] 2018 SB 56 created the Kansas Cybersecurity Act (Act). The Act established the position of Executive Branch CISO, who will serve as the Executive Branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance, and technologies impacting Executive Branch cybersecurity programs. The CISO will also coordinate cybersecurity efforts among Executive Branch agencies and provide guidance when personal information or computer resources have been compromised or are likely to be compromised due to a high-risk threat or vulnerability. The Act also established the Kansas Information Security Office (KISO) within the Office of Information Technology Services to effect the provisions of the Act. The KISO will be under the direction of the CISO.

The Act directed Executive Branch agency heads be solely responsible for security of all data and IT resources under such agency's purview, irrespective of the location of the data or resources and must implement policies and standards to ensure all the agency's data and IT resources are maintained in compliance with applicable state and federal laws, rules, and regulations. Agency heads must also ensure an agency-wide IS program is in place and designate an IS officer to administer the agency's IS program who reports directly to executive leadership. Participation in annual agency leadership training concerning cybersecurity and CISO-sponsored statewide cybersecurity program initiatives and services is required of agency heads as well. Appropriate and cost-effective safeguards must be implemented to reduce, eliminate, or recover from identified threats to data and IT resources. Agency heads are required to ensure the agency conducts annual internal assessments of its security programs. A cybersecurity assessment report must be submitted to the CISO in even-numbered years and a summary of the cybersecurity assessment report must be submitted to the House Committee on Government, Technology and Security, or its successor committee, and the Senate Committee on Ways and Means.

2018 HB 2359.[51] The bill, which incorporated the contents of HB 2333 and SB 264, amended the qualifications for candidacy for several statewide elected offices, created law requiring manual audits of elections, amends law related to the timing of the election canvasses and to electronic voting machines, and amended provisions in election law concerning signatures if the voter has a disability that prevents the individual from signing.

Kansas Work with the Federal Government

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 the National Cybersecurity and Communications Integration Center (NCCIC), which helps 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.[52] Eleven states, including Kansas, chose not to accept DHS' offer, citing concerns with federal intrusion on state elections.[53]

On January 6, 2017, the Secretary of DHS determined election infrastructure should be designated as a critical infrastructure sub-sector.[54] 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 voluntary security assistance. 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.[55]

Federal and State Election Security Funding

Federal Funding. HAVA, enacted in 2002, addressed improvements to voting systems and voter access identified following the 2000 election. HAVA required states implement the following new programs and procedures:

- Provisional voting;
- Voting information;
- Updated and upgraded voting equipment;
- Statewide voter registration databases;
- Voter identification procedures; and
- Administrative complaint procedures.

Kansas received $26.4 million in total HAVA funds and has $2.9 million remaining as of early 2018.

On March 23, 2018, the Consolidated Appropriations Act of 2018 (Act) was signed into law.[56] 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 2018 HAVA Election Security Fund marks the first new appropriations for HAVA grants since FY2010. Consistent with the requirements of HAVA, states may use this funding to:

- Replace voting equipment that only records a voter's intent electronically with equipment that utilizes a voter verified paper record;

- Implement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally;

- Upgrade election-related computer systems to address cyber vulnerabilities identified through Department of Homeland Security, or similar scans or assessments of, existing election systems;

- Facilitate cybersecurity training for the state chief election official's office and local election officials;

- Implement established cybersecurity best practices for election systems; and

- Fund other activities that will improve the security of elections for Federal office.

States received grant award notification letters from the EAC in April 2018. The letter allowed states to incur costs, with prior EAC approval, against the forthcoming grant awards, effective the date of the notification letter. States are required to match 5.0 percent of the funds awarded within two years of receiving federal funds.

The SOS submitted the request for the funds on June 27, 2018, and as of July 16, 2018, all 50 states had submitted requests for the funds. Kansas will receive $4,383,595 in 2018 HAVA funds, and will have a match amount of $219,180.[57]

State Funding. The SOS budget totals $4.5 million for FY2018 and $4.6 million for FY2019, all from special revenue funds.[58] The SOS budgeted $548,977 for elections and legislative matters for FY 2018 and $551,359 for FY 2019.

CASE STUDY: COLORADO

Colorado was one of the 21 states targeted by hackers during the 2016 Presidential Election.[59] However, recently, Colorado has received praise for the security of its election systems and was one of 11 states that received a B ranking from CAP. The State earned high marks for the use of the vote by mail system; the use of risk-limiting audits; and its adherence to a number of minimum cybersecurity best practices for voter registration systems. Also, a 2015 Brookings Institution study showed Colorado was one of only two states, along with New Mexico, demonstrating a "solid and robust" understanding of the importance of integrating cybersecurity in its strategic IT plan.[60] The Secure Colorado Strategic Plan developed by the Governor's Office of Information Technology received awards from the National Association of State CIOs, the Center for Digital Government, and CSO Magazine.

Online Voter Registration System

Colorado has updated their voter registration system within the last ten years. The voter registration system provides access control to ensure that only authorized personnel has access to the database. The State also uses logging capabilities to track modifications to the database, an intrusion detection system, and performs regular vulnerability assessments and penetration testing on the voter registration system. All election administrators – at state, local, and municipal levels – receive cybersecurity training prior to using the voter registration system and receive ongoing training quarterly. Colorado offers anti-malware endpoint protection software, at no cost to users, to monitor and defend against election day attacks.

Electronic Poll Book

CRS 1-5-302 provides county clerk and recorders the ability to use EPBs. A single electronic poll book, which is built into the State's voter registration database, is used at all vote centers and is tested prior to each election. Many counties provide backup paper voter registration lists, however, there is no requirement to do so. If an EPB fails, all voters would shift to provisional ballots, which would be checked against the voter registration system once it is restored.

Election Personnel

In accordance with CRS 24-72-305.6, all permanent and temporary county staff and all vendor staff who have access to the voting system or any voting or counting equipment must pass a criminal background check.

Voting Devices

While the State primarily uses a vote by mail system, there are a limited number of DRE devices in use at vote centers.[x] These machines are required to use VVPAT, as per CRS 1-5-801, and are not connected to the internet. Colorado, like Kansas, also requires that voting devices be tested to EAC Voluntary Voting System Guidelines before being purchased and election officials carry out pre-election logic and accuracy testing on all machines.[61] Colorado SOS Wayne Williams stated voting equipment is kept in a locked room with surveillance and a log of who accesses the room.[62]

Storage and Tallying of Votes

Central count centers are required to review and account for all voting machine memory cards and flash drives to ensure they have been properly loaded into the tally server. Central count centers are also required to compare and reconcile voter center totals with countywide results to ensure they add up to the correct total. Colorado requires all election results and reconciliation procedures be made public. The computers used to tabulate the results are not allowed to be connected to the internet. Results are transferred from the offline computers to another system, which uploads the tallies to the SOS. The only election officials and judges who have access to the tabulation process must first pass a Colorado Bureau of Investigation background check and the tabulation computers also track who has accessed information, down to the keystroke.[63]

Post-election audits

The Colorado Legislature ordered the use of risk-limiting audits in 2009, [CO Rev Stat § 1-7-515], making Colorado the first state to require risk-limiting audits after every election. The state also became the first to complete a statewide risk-limiting audit in 2017. The procedures for conducting risk-limiting audits are spelled out in SOS Election Rule 25.[64]

---

[x] Colorado statutes concerning electronic voting devices can be found in CO Rev Stat § 1-5-601.

Other Election Security Resources

Cyber Liability Insurance. In March 2018, the Colorado Legislature passed HB 18-1128, which required the Colorado Department of Personnel and Administration (DPA) to purchase a cybersecurity insurance policy that will cover all state agencies in FY 2018-2019.[65] This policy will have an annual premium of $325,000 and coverage up to $5.0 million per incident. This includes crisis mitigation, incident response, *i.e.* providing notifications, data recovery, and annual cybersecurity training for state agencies. Beginning in FY 2018-2019, state agencies would pay their portion of the policy through reappropriated funds to DPA.

White-hat hackers. Currently, it does not appear that the Colorado SOS utilizes white-hat hackers.

Interstate Information Sharing. Colorado is a member of the MS-ISAC. Eighteen counties and the Colorado SOS are members of EI-ISAC.

Albert. The Colorado SOS utilizes Albert. However, further information was not provided.

The Athenian Project. According to a representative, there are Colorado government entities that use the Project. However, they were unable to provide further information.

Project Shield. KLRD was unable to obtain information on whether the Colorado SOS works with Shield.

Colorado Work with the Federal Government

Colorado was one of seven states that participated in DHS "cyber storm," the nation's largest cybersecurity exercise, along with nearly 1,000 other players across the nation, ranging from law enforcement agencies to transportation and manufacturing networks.[66] Colorado has also established contingency plans in case of an emergency. The Colorado National Guard is present at the SOS office on election day in case any problems arise to help resolve any possible situation.[67]

Federal and State Election Security Funding

Federal Funding. Colorado received $20.2 million original HAVA funds in total and has $517,949 remaining.[68] The State requested the 2018 HAVA funds on June 8, 2018, and received $6.3 million, with a $317,149 match.

State Funding. The Colorado SOS has a budget of almost $23.0 million for FY 2017-2018 and almost $25.4 million for FY 2018-2019, all from special revenue funds. The SOS estimates about 60.0 to 70.0 percent of the budget is dedicated to the administration of elections.[69]

GLOSSARY

- *Application whitelisting* - allows only specified programs to run while blocking all others, including malicious software.

- *Botnets* - a string of connected computers coordinated together to perform a task. That can mean maintaining a chatroom, or it can be taking control of your computer.

- *Bug bounty* - a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.

- *Business continuity* - a concept that refers to the planning and preparation of a company to make sure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short period.

- *Cache* - a hardware or software component that stores data so future requests for that data can be served faster; the data stored in a cache might be the result of an earlier computation, or the duplicate of data stored elsewhere.

- *Cross-site scripting (XSS) vulnerability* - allows threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on voter registration websites can provide the attacker unauthorized access to voter information.

- *Denial-of-service (DoS) attack* - prevents legitimate users from accessing information or services. A DoS attack can make a voter registration website unavailable or deny access to voter registration data.

- *Distributed denial of service (DDoS) attack* - a type of DoS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a DoS attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. A DoS attack is different from a DDoS attack. The DoS attack typically uses one computer and one internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.

- *Injection flaw* – 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. The most common example is Structured Query Language (SQL) injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the voter registration database. Another form is Command Injection, where an untrusted user is able to send commands to an operating systems supporting a web application or database.

- *Input validation* - a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and Command Injection.

- *Intrusion Detection System (IDS)* - a device or software application that monitors a network or systems for malicious activity or policy violations.

- *Penetration testing* - an authorized simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify both vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

- *Phishing attack* - includes forged emails, texts, and other messages used to manipulate users into clicking on malicious links or downloading malicious file attachments. Phishing attacks can lead to credential theft (e.g., passwords) or may act as an entry point for threat actors to spread malware throughout an organization, steal voter information, or disrupt voting operations.

- *Proxy server* - a go-between or intermediary server that forwards requests for content from multiple clients to different servers across the internet.

- *Ransomware* - 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. Affected organizations are discouraged from paying the ransom, as this does not guarantee access will be restored to a compromised voter registration database.

- *Reverse proxy* - a type of proxy server that typically sits behind the firewall in a private network and directs client requests to the appropriate backend server. A reverse proxy provides an additional level of abstraction and control to ensure the smooth flow of network traffic between clients and servers.

- *Secure sockets layer security (SSL)* - 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. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

- *Trojan horse (Trojan)* - a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

- *White-hat hacker* - a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them.

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 Arkin, William; Dilanian, Ken; McFadden, Cynthia. (2018, February 28). U.S. Intel: Russia Compromised Seven States Prior to 2016 Election. Retrieved from https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296

3 US-CERT. (2016, September 30). Security Tip (ST16-001) Securing Voter Registration Data. Retrieved from https://www.us-cert.gov/ncas/tips/ST16-001

4 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

5 Center for Internet Security. (2018, March 15). A Handbook for Elections Infrastructure Security, Part 2: Election Systems and Risk. Retrieved from https://www.cisecurity.org/best-practices-part-2/

6 U.S. Election Assistance Commission. E-Pollbook Requirements. Retrieved from https://www.eac.gov/voting-equipment/e-pollbook-requirements/

7 Reinicke, Carmen. (2018, June 21). The Biggest Cybersecurity Risk to US Businesses is Employee Negligence, Study Says. Retrieved from https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html?wpisrc=nl_cybersecurity202&wpmm=1

8 Election Assistance Commission. (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 Election Assistance Commission. (2017, September 12). Voluntary Voting System Guidelines 2.0. Retrieved from https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

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 https://icitech.org/icit-analysis-hacking-elections-is-easy-partone-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 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/

14 Kirby, Jen. (2018, May 8). Why It Takes So Long to Get Election Night Results. Retrieved from https://www.vox.com/2018/5/8/17320758/primary-election-night-results-ohio-west-virginia-indiana-north-carolina

15 NCSL. (2018, July 15). Post-Election Audits. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx

16 American Statistical Association. (2010, April 17). American Statistical Association Statement on Risk-Limiting Post-Election Audits. Retrieved from http://www.amstat.org/asa/files/pdfs/POL-Risk-Limiting_Endorsement.pdf

17 NCSL. (2018, July 15). Post-Election Audits. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx

18 National Association of State Procurement Officials. (2016). Cyber Liability Insurance 101. Retrieved from https://www.naspo.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=16&moduleid=8806&articleid=3403&documentid=261

19 Verisk. (2018, March 19). ISO's New Cyber Insurance Program Implemented in 42 States and U.S. Territories. Retrieved from https://www.verisk.com/press-releases/2018/march/isos-new-cyber-insurance-program-implemented-in-42-states-and-us-territories/

20 National Association of State Procurement Officials. (2016). Cyber Liability Insurance 101. Retrieved from https://www.naspo.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=16&moduleid=8806&articleid=3403&documentid=261

21 Bergal, Jenni. (2017, November 10). Worried About Hackers, States Turn to Cyber Insurance. Retrieved from http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/11/10/worried-about-hackers-states-turn-to-cyber-insurance

22 Bergal, Jenni. (2018, May 14). White-Hat Hackers to the Rescue. Retrieved from http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/05/14/white-hat-hackers-to-the-rescue

23 Center for Internet Security. What is an ISAC. Retrieved from https://www.cisecurity.org/isac/

24 Center for Internet Security. MS-ISAC Membership FAQ. Retrieved from https://www.cisecurity.org/ms-isac/ms-isac-membership-faq/
25 Center for Internet Security. EI-ISAC Membership FAQ. Retrieved from https://www.cisecurity.org/ei-isac/ei-isac-membership-faq/
26 Wright, M. (2018, July 16). Trump and Putin Should Be Talking About Cyber Weapons and Social Media Instead of Nuclear Weapons. Retrieved from http://thehill.com/opinion/cybersecurity/397120-Trump-and-Putin-should-be-talking-about-cyber-weapons-and-social-media-instead-of-nuclear-weapons
27 Center for Internet Security. Albert. Retrieved from https://www.cisecurity.org/services/albert/
28 Leonard, Matt. (2018, March 28). Sensor Network Protects Voter Registration Sites. Retrieved from https://govcyberinsider.com/articles/2018/03/30/albert-intrusion-detection-voter-registration.aspx
29 Cloudflare. (2017). Athenian Project. Retrieved from https://www.cloudflare.com/athenian/
30 Masterson, Matthew. (2018, February 15). A Coordinated Response to Protect American Elections. Retrieved from https://www.eac.gov/a-coordinated-response-to-protect-american-elections-/
31 Cloudflare. (2017). Athenian Project. Retrieved from https://www.cloudflare.com/athenian/#qualifications
32 Ng, Alfred. (2018, May 16). Google Rolls Out Free Cyberattack Shield for Elections and Campaigns. Retrieved from https://www.cnet.com/news/google-rolls-out-free-project-shield-cyberattack-protection-for-elections-and-campaigns/
33 Kennedy, L.; Parshall, J.; Root, D.; Sozan, M. (2018, February 12). Election Security in All 50 States. Retrieved from https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/
34 Office of the Secretary of State. (2004, March). Voting System Security Policy. Retrieved from https://www.sos.ks.gov/other/voting_security_policy.html
35 NCSL. (2017, December 6). Online Voter Registration. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx
36 Lowery, B. (2016, September 1). Kansas Works with Feds, Other States to Keep Voter Data Secure. Retrieved from http://www.govtech.com/pcio/articles/Kansas-Works-with-Feds-Other-States-to-Keep-Voter-Data-Secure.html
37 Kansas Office of the Governor, Office of Information Technology Services. (2014, December 1). Information Security Policies, Procedures and Baselines. Retrieved from http://oits.ks.gov/docs/default-source/policydocumentslibrary/p9209-oits-information-security-policy.pdf?sfvrsn=2
38 Koranda, S. (2016, September 6). Kobach Confident in Security of Kansas Voter Registration Data. Retrieved from http://kmuw.org/post/kobach-confident-security-kansas-voter-registration-data
39 NCSL. (2017, March 22). Electronic Poll Books, E-Poll Books. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx
40 Hammill, R. (2016, April 26). Will Johnson County Be Ready for the 2016 Presidential Election? Retrieved from https://www.kansascity.com/news/local/community/joco-913/article74045762.html
41 KSA 25-2804. Retrieved from http://www.ksrevisor.org/statutes/chapters/ch25/025_028_0004.html
42 Verified Voting. (2016) The Verifier – Polling Place Equipment – November 2016. Retrieved from https://www.verifiedvoting.org/verifier/#year/2016/state/20
43 KSA 25-4406(k). Retrieved from http://www.ksrevisor.org/statutes/chapters/ch25/025_044_0006.html
44 KSA 25-4407(b). Retrieved from http://www.ksrevisor.org/statutes/chapters/ch25/025_044_0007.html
45 Office of the Secretary of State. (2004, March). Voting System Security Policy. Retrieved from https://www.sos.ks.gov/other/voting_security_policy.html
46 Shorman, J. (2018, February 18). Report: Kansas Gets Failing Election Security Grade. Retrieved from http://www.govtech.com/security/Report-Kansas-Gets-Failing-Election-Security-Grade.html
47 Eveld, E. (2016, January 25). Kris Kobach proposes voting-machine audits, files new voter fraud cases. Retrieved from https://www.kansascity.com/news/politics-government/article56474273.html
48 KLRD. (2018). 2018 Legislative Summary. Retrieved from http://www.kslegislature.org/li/b2017_18/measures/documents/summary_hb_2539_2018.pdf
49 CIS. (2018). EI-ISAC Members. Retrieved from https://www.cisecurity.org/ei-isac/partners-ei-isac/
50 KLRD. (2018). 2018 Legislative Summary. Retrieved from http://www.kslegislature.org/li/b2017_18/measures/documents/summary_sb_56_2018.pdf
51 KLRD. (2018). 2018 Legislative Summary. Retrieved from http://www.kslegislature.org/li/b2017_18/measures/documents/summary_hb_2539_2018.pdf
52 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
53 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/

54 DHS. (2017, January 6). Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as Critical Infrastructure Subsector. Retrieved from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

55 Kansas City Star Editorial Board. (2018, March 22). Are Kansas and Missouri making sure this year's elections are secure from meddling? Retrieved from https://www.kansascity.com/latest-news/article206315564.html

56 EAC. (2018, March 30). 2018 HAVA Election Security Funds. Retrieved from https://www.eac.gov/2018-hava-election-security-funds/

57 EAC. (2018, March 30). HAVA Funds State Chart View. Retrieved from https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/

58 KLRD. (2018, July). Fiscal Facts. Retrieved from http://www.kslegresearch.org/KLRD-web/Publications/FiscalFacts/2018_fiscal_facts.pdf

59 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

60 Stapleman, J. Award-winning cybersecurity plan guards Colorado's electronic data. Retrieved from https://www.colorado.gov/pacific/cdphe/news/cybersecurity

61 Colorado SOS. (2017, December 7). Election Rules [8 CCR 1505-1]. Retrieved from https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule11.pdf

62 Walker, C. (2018, April 15). Colorado's Election Systems Are Being Hacked...on Purpose, by the Feds. Retrieved from https://www.westword.com/news/department-of-homeland-security-testing-colorados-election-systems-with-operation-cyber-storm-10197655

63 Minor, N. (2016, October 20). It Would Be Really Hard To 'Rig' Colorado's Election System. Here's Why. Retrieved from http://www.cpr.org/news/story/it-would-be-really-hard-to-rig-colorados-election-system-heres-why

64 Colorado SOS. (2018, March 26). Election Rules [8 CCR 1505-1], Rule 25. Post-election audit. Retrieved from http://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule25.pdf

65 Colorado General Assembly. (2018, May 29). Protections For Consumer Data Privacy. Retrieved from https://leg.colorado.gov/bills/hb18-1128

66 Walker, C. (2018, April 15). Colorado's Election Systems Are Being Hacked...on Purpose, by the Feds. Retrieved from https://www.westword.com/news/department-of-homeland-security-testing-colorados-election-systems-with-operation-cyber-storm-10197655

67 Sunny, J. (2018, April 26). Colorado praised for election security. Retrieved from https://bartels-on.sos.state.co.us/index.php/2018/04/26/colorado-praised-for-election-security/

68 Colorado SOS. (2003, May 29). State of Colorado Help America Vote State Plan. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwjpqKvGjMDcAhVObK0KHaMZDIUQFjAHegQIARAC&url=https%3A%2F%2Fwww.sos.state.co.us%2Fpubs%2Felections%2FHAVA%2Ffiles%2Fhavastateplanv302fr.pdf&usg=AOvVaw0Xb0IlPR_4PlxfBFs668iF

69 Colorado Joint Budget Committee. (2018). Appropriations Report Fiscal Year 2018-2019. Retrieved from http://leg.colorado.gov/sites/default/files/fy18-19apprept_0.pdf