KLRD

Jessa Farmer
Research Analyst
785-296-4409
Jessa.Farmer@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 federal U.S. 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, postelection audits, and other cybersecurity tools.

Online Voter Registration Systems

The EAC found more than 211 million registered voters for the 2018 election. According to the National Conference of State Legislatures (NCSL), currently 40 states and the District of Columbia (D.C.) use an online voter registration system to register those voters. Additionally, Oklahoma is phasing in online voter registration as of late 2020. 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 during the 2016 election. While Arizona, Florida, and Illinois were confirmed to have breaches of their voter registration systems, a 2018 NBC News article[1] indicated four other states' voter registration systems were compromised to varying levels of severity before the 2016 election. To date, no evidence has been found that any voter information was altered or deleted.

The Kansas 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 a firewall was

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 that the voter registration system had logging capabilities to track modifications to the database.

Electronic Poll Books

In January 2014, the Presidential Commission on Election Administration recommended all jurisdictions transition to electronic poll books (EPBs). The EAC indicates 36 states and the District of Columbia (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 made 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. The Center for Internet Security 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. Some ways in which EPBs can be secured include the use of secure sockets layer security,[2] use of a virtual private network,[3] and proper security training for staff.

Vote Centers

EPBs are generally used in states that allow or require the use of vote centers. Vote centers are an alternative to specific precinct polling places and allow any voter to cast a ballot in any vote center in the jurisdiction (generally a county) rather than at their assigned polling place. States that allow or require the use of vote centers also generally allow or require local jurisdictions to use EPBs, which can be used to receive immediate updates on voters who have voted in other vote centers (unless the state specifies that the EPB may not be connected to the network).

In 2019, Kansas law was amended with enactment of Sub. for SB 130, permitting all voters in a county to vote at any polling place on election day, at the discretion of the county voting official.

According to NCSL, as of 2020, 16 states statutorily allow the use of vote centers as an alternative to precinct polling places.[4] Of those 16 states: 7 require counties to use EPBs, 5 states allow counties to use EPBs, and 4 states (Kansas included) do not specify in statute whether the county is required or permitted to use EPBs."

Postelection Audits

Currently, 38 states and the District of Columbia (D.C.) require some form of a postelection audit.

NCSL has divided postelection audits into two categories:

- Traditional postelection audit: usually conducted 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-four states[5] and the District of Columbia (D.C.) require a traditional postelection audit, and

Colorado, Nevada, Rhode Island, and Virginia statutorily require risk-limiting audits.

In Kansas, 2018 HB 2539 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 (KSA 25-3009).

The Office of the Secretary of State selected the random offices to be audited from the 2020 general election on November 4, 2020.

Electronic Transmission of Ballots

The EAC reported The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters are increasingly using electronic means to receive and return absentee ballots. email 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* email. Voting securely through the Internet places much of the security responsibility on the votes 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.

According to NCSL, 4 states allow certain voters to return ballots using a web-based portal, 19 states and D.C. allow certain voters to return ballots *via* email or fax, 7 states allow certain voters to return ballots *via* fax, and 19 states do not allow electronic transmission and permit voters to return ballots only through postal mail.[6]

Additionally, in 2018, West Virginia began using a block chain-enabled mobile voting application, called Voatz, for overseas residents from 24 counties. However, it suspended use of that application for the 2020 elections.

Other Election Security Resources

States utilize a myriad of resources to protect their election infrastructure from outside attacks. These resources may include cyber-liability insurance,[7] enlisting the help of the National Guard and white-hat hackers,[8] participation in interstate information sharing programs,[9] and cybersecurity services provided by either the federal government or private entities.[10]

Current Federal Government Activities

The Department of Homeland Security (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 collocated 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, the 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 through the DHS Cybersecurity and Infrastructure Security Agency (CISA).

DHS was attempting to obtain security clearances for the top election official in each state so those officials would 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. According to a report from the Office of the Inspector General dated February 2019 on an audit conducted to evaluate the effectiveness of DHS' efforts to coordinate with states to secure election infrastructure, the lengthy security clearance process hinders DHS' efforts to secure the election infrastructure.

Initially, only 19 states signed up for the risk assessments DHS offered, and 14 conducted "cyber-hygiene" scans. In the Office of the Inspector General audit report, it was noted state and local officials' mistrust of federal involvement increased reluctance to request DHS assistance. The audit noted CISA performed weekly cyber-hygiene scans on 141 outward facing election networks and conducted 35 risk and vulnerability assessments for election stakeholders. An October 2020 Inspector General audit report noted CISA had increased its outreach to and coordination with election stakeholders. The CISA National Risk Management Center (Center) focuses on evaluating threats and defending critical infrastructure against hacking. The Center runs simulations, tests, and cross-sector exercises to evaluate critical infrastructure weaknesses and threats.

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

On February 20, 2018, the U.S. Attorney General ordered the creation of the Department of Justice (DOJ) Cyber-Digital Task Force (Task Force) to canvass the ways the DOJ addresses the global cyber threat and identify how federal law enforcement can more effectively accomplish its mission in this area.

The Attorney General has asked the Task Force to prioritize its study of efforts to interfere with U.S. elections. The Task Force released a report on July 19, 2018. The DOJ also issued a statement indicating the agency planned to alert American companies, private organizations, and individuals they are being covertly attacked by foreign actors attempting to affect elections or the political process. The Task Force has released several reports focusing on cyber threats, including malign foreign influence operations and potential threats relating to the use of cryptocurrency.

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, the Central Intelligence Agency, and DHS and continues to generate insight on foreign adversaries to improve cyber defenses. DHS created the National Risk Management Center (NRMC) within the Cybersecurity and Infrastructure Agency; it is a centralized location for government and private

sector partners to share information related to digital security.

In August 2018, DHS, EAC, DOD, the National Institute of Standards and Technology, NSA, Office of the Director of National Intelligence, U.S. Cyber Command, DOJ, the FBI, 44 states (including Kansas), D.C., and numerous counties participated in the Tabletop the Vote 2018, DHS' National Election Cyber Exercise 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 to interfere or to have interfered with U.S. election processes or equipment.

EAC Current Activities

The EAC recommended the Voluntary Voting Systems Guidelines (VVSG) Version 2.0 in September 2017. The VVSG Version 2.0 states a voting device must produce a voter verifiable paper audit trail (VVPAT), and the software or hardware cannot produce errors that could lead to undetectable changes in tallies. The VVSG Version 2.0 voluntary requirements were released in February 2020. The EAC has also added a page to its website concerning election security preparedness, with many links to information on how to secure election systems, guides on what to do during and after a cybersecurity incident, and glossaries for commonly used terms (*https://www.eac.gov/election-officials/election-security-preparedness*).

New Help America Vote Act (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 was for election cybersecurity and to purchase new voting equipment.

In 2018, Congress appropriated $4.3 million for election security in Kansas, requiring a 5 percent match that was met by a Kansas State General Fund (SGF) transfer in FY 2019 and FY 2020. In 2019, Congress appropriated an additional $4.6 million for election security in Kansas under the Act, requiring a 20 percent match that was met by SGF moneys for FY 2021.

In August 2020, the EAC notified the Kansas Secretary of State (Secretary) an additional $15,427 appropriation for election security would be added to the original appropriation, requiring a $3,085 match. The Secretary requested this state match as a SGF transfer in FY 2022.

The EAC allowed states to combine funds into one fund titled "2018 HAVA Election Security," and the total award for Kansas is approximately $9.3 million. Such funds do not have an expiration date for expenditure.

HAVA CARES Act Funding

In response to the COVID-19 pandemic, in March 2020, the Coronavirus Aid, Relief and Economic Security (CARES) Act was enacted and appropriated $400.0 million in HAVA funds to states to prevent, prepare for, and respond to the COVID-19 pandemic for the 2020 federal election cycle. Such funding is separate from the 2018 and 2020 HAVA election security funding.

Kansas was awarded approximately $4.6 million of the total $400.0 million in funding. Such appropriation must be used by December 31, 2020, and Kansas must provide a 20 percent match by March 2022. The required state match for Kansas is $924,500.

The Kansas Secretary of State announced the following plan for the expenditure of HAVA CARES Act funding:

- Approximately $2.6 million to reimburse all 105 counties for COVID-19-related

expenditures, according to a formula based on voting age population for each county's allotted reimbursement cap. No county received a reimbursement allotment cap of less than $5,000. Counties submitted plans in May 2020 for such funds and have until December 2020 to submit receipts to the Secretary for reimbursement;

- Approximately $1.0 million to procure personal protection equipment kits, plexiglass shields, and disposable pens for voters and polling places statewide to ensure additional protection for election workers and voters;
- Approximately $365,000 to purchase secure drop boxes for mail ballots. The Secretary authorized such funds to purchase two secure drop boxes per county, with certain exceptions;
- Approximately $150,000 to publish targeted, digital educational ads to all registered voters in the state for the general election to educate voters on options to cast a ballot in the November 2020 election amidst the COVID-19 pandemic; and
- A small portion of such funds to establish improved teleconferencing and telework options for election-related items, including virtual election panels and media opportunities.

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[11] that received an unsatisfactory ranking. However, 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 postelection 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 "Postelection 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.

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 direct-recording electronic voting machines (DREs) without VVPAT, 57 DREs with VVPAT, 4,461 ballot marking devices, and 953 electronic scanners. As of March 2018, approximately 20 counties had replaced some or all of their voting devices or were in the process of purchasing new voting devices, including Johnson County.

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(m) requires voting devices to be compliant with HAVA voting system standards. Logic and accuracy testing must be conducted on all voting devices within 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.

Amendments to KSA 25-4406 in 2018 HB 2539 require any electronic or electromechanical voting system approved by the Secretary of State 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 Vote Tallies

KAR 7-21-2 states results are to be sent only by fax, phone, hand delivery, or encrypted electronic transfer. According to the Office of the Secretary of State, officials typically call in or email results, and there is no Internet uploading of results.

COVID-19 Pandemic-Related Information

In June 2020, the Brennan Center released "Preparing for Cyberattacks and Technical Problems During the Pandemic," which included a checklist for election officials to navigate cybersecurity during the COVID-19 pandemic.[12] The checklist includes instructions for election administration and infrastructure; mail voting; in-person voting; and results reporting, certification, and public communications.

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/Elections&Ethics.html.

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-intelrussia-compromised-seven-states-prior-2016-election-n850296.
2 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.
3 A virtual private network creates a safe and encrypted connection over a less secure network.
4 NCSL, *Vote Centers*, https://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx
5 Alaska, Arkansas, Arizona, California, Connecticut, Delaware, 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.
6 NCSL, *Electronic Transmission of Ballots*, https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.
7 Cyber-liability insurance is coverage for financial consequences of electronic security incidents and data breaches.
8 A white-hat hacker is a computer security specialist who breaks into protected systems and networks for potential improvements.

9 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.

10 Cybersecurity services are provided by private entities including The Athenian Project and Project Shield.

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

12 The Brennan Center for Justice, *Preparing for Cyberattacks and Technical Problems During the Pandemic*. *https://www.brennancenter.org/our-work/research-reports/preparing-cyberattacks-and-technical-problems-during-pandemic-guide*.

For more information, please contact:

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

KLRD

Robert Gallimore
Managing Research Analyst
785-296-4420
Robert.Gallimore@klrd.ks.gov

Elections and Ethics

D-2 Kansas Open Meetings Act

Purpose

The Kansas Open Meetings Act (KOMA), KSA 75-4317, *et seq.*, recognizes "that a representative government is dependent upon an informed electorate" and declares the policy of the State of Kansas is one where "meetings for the conduct of governmental affairs and the transaction of governmental business be open to the public."

The Kansas Supreme Court has recognized KOMA is to be "interpreted liberally and exceptions narrowly construed" to carry out the purpose of the law. [*Mem'l Hosp. Ass'n v. Knutson*, 239 Kan. 663, 669 (1986)]

State and Local Public Bodies Covered by KOMA

- State agencies;
- Political and taxing subdivisions of the state;
- Legislative bodies of the state or its subdivisions;
- Administrative bodies of the state or its subdivisions;
- Boards, commissions, authorities, councils, committees, and subcommittees of the state or its subdivisions, or of legislative or administrative bodies thereof; and
- Other subordinate groups of any of the above entities that receive or expend and are supported in whole or in part by public funds (KSA 75-4318).

State Bodies Covered by KOMA

- The Legislature and its legislative committees and subcommittees, unless rules provide otherwise;
- State administrative bodies, boards, and commissions;
- State Board of Regents;
- State Board of Education;
- Kansas Turnpike Authority;
- Supreme Court Nominating Commission (added by 2016 SB 128); and
- Other state bodies.

Local Governments Covered by KOMA

The following local governments are covered by KOMA:

- Cities;
- Drainage districts;
- Counties;
- Conservation districts;
- School districts;
- Irrigation districts;
- Townships;
- Groundwater management districts;
- Water districts;
- Watershed districts;
- Fire districts;
- Municipal energy agencies;
- Sewer districts;
- District judicial nominating commissions (added by 2016 SB 128); and
- Other special district governments.

Public Bodies Excluded from KOMA

Certain state and local bodies or entities are excluded from the requirements of KOMA, including the following:

- The Judicial Branch (except for judicial nominating commissions);
- State or local bodies when exercising quasi-judicial powers (examples include teacher due process hearings, civil service board hearings for a specific employee, or zoning amendment hearings for a specific property); and
- Certain state bodies when performing functions that are exempt from KOMA by statute (examples include committee discussion on certain Secretary of Commerce decisions regarding sales tax and revenue (STAR) bonds).

Meetings: What are They?

KOMA covers meetings, which are defined in KSA 75-4317a as a gathering or assembly with the following characteristics:

- Occurs in person or through the use of a telephone or any other medium for "interactive" communication (see the following "Serial Meetings" section);
- Involves a majority of the membership of an agency or body; and
- Is for the purpose of discussing the business or affairs of the body. The Kansas Court of Appeals has held that informal discussions before, after, or during recesses of a public meeting are subject to the requirements of the open meetings law. [*Coggins v. Pub. Emp. Relations Bd*, 2 Kan. App. 2d 416 (1978)] Calling a gathering a "work session" does not exempt the event from the law if the three requirements of a meeting are met.

Social gatherings are not subject to KOMA as long as there is not a majority of the membership present or there is no discussion of business of the public body between a majority of the membership.

Serial Meetings

The Attorney General has said serial communications among a majority of a quorum of a public body constitute a meeting if the purpose is to discuss a common topic of business or affairs of that body by the members.

Such a meeting may occur through calling trees, email, or the use of an agent (staff member) of the body (Att'y. Gen. Op. 98-26 and 98-49).

The use of instant messaging also would qualify as a meeting. KSA 75-4318(f) now deems interactive communications in a series to be subject to open meetings requirements if the communications:

- Collectively involve a majority of the membership of the body or agency;

- Share a common topic of discussion concerning the business or affairs of the body or agency; and
- Are intended by any or all of the participants to reach agreement on a matter that would require binding action to be taken by the body or agency.

Is Binding Action the Trigger?

In regard to discussing "the business or affairs of the body," binding action or voting is not necessary. It is the discussion itself that triggers the requirements of KOMA (KSA 75-4317a).

Notice of Meetings, Agendas, Minutes, Conduct of Meeting, and Cameras

Notice Required Only When Requested

KOMA does not require notice of meetings to be published. According to KSA 75-4318(b), notice must be given to any person or organization requesting it. Notice requests may expire at the end of a fiscal year, but the public body has a duty to notify the person of the pending expiration before terminating notice. The presiding officer has the duty to provide notice, but that duty may be delegated. No time limit is imposed for receipt of notice prior to the meeting.

Notice may be given in writing or orally, but it must be made individually to the person requesting it. Posting or publication in a newspaper is insufficient. A single notice can suffice for regularly scheduled meetings. There is also a duty to notify of any special meetings. No fee for notice may be charged.

Petitions for notice may be submitted by groups of people, but notice need be provided only to one person on the list, that person being designated as required by law. All members of an employee organization or trade association are deemed to have received a notice if one is furnished to the executive officer of the organization.

Agenda Not Required

KSA 75-4318(d) states, "Prior to any meeting…, any agenda relating to the business to be transacted at such meeting shall be made available to any person requesting the agenda." In *Stevens v. City of Hutchinson*, 11 Kan. App. 2d 290 (1986), the court concluded while the law does not require an agenda be created, if a body chooses to create an agenda, the agenda should include topics planned for discussion.

Requirements for Minutes

The only KOMA requirement for minutes pertains to closed or executive sessions. KSA 75-4319(a) requires any motion to recess for a closed or executive meeting be recorded in the meeting minutes. (See "Executive Sessions: Procedure and Subjects Allowed" on the following page for additional information.)

Conduct of Meetings

Any person may attend open meetings, but the law does not require the public be allowed to speak or have an item placed on the agenda. KOMA does not dictate the location of a meeting, the size of the room used (or even that a room must be used) or other accommodation-type considerations. The court has determined (see *Stevens*) a meeting is "open" if it is accessible to the public.

KSA 75-4318(a) prohibits the use of secret ballots for any binding action. The public must be able to ascertain how each member voted.

Use of Cameras

Subject to reasonable rules, cameras and recording devices must be allowed at open meetings (KSA 75-4318(e)).

Executive Session: Justification and Procedure

Pursuant to KSA 75-4319, only a limited number of subjects may be discussed in executive session. Some of these are listed below.

Personnel Matters of Non-elected Personnel

The purpose of this justification is to protect the privacy interests of individuals. Discussions of consolidation of departments or overall salary structure are not proper topics for executive session. This personnel justification applies only to employees of the public agency. The Attorney General has opined the personnel justification does not apply to appointments to boards or committees, or nomination of public officers, nor does it apply to independent contractors (Att'y. Gen. Op. 2016-03).

Consultation with an Attorney

For the body or agency to be deemed privileged in the attorney client relationship, all elements of privilege must be present:

- The body's attorney must be present;
- The communication must be privileged; and
- No other third parties may be present.

Additional Justifications

Additional justifications for executive session are as follows:

- Employer-employee negotiations to discuss conduct or status of negotiations, with or without the authorized representative who actually is doing the bargaining;
- Confidential data relating to financial affairs or trade secrets of corporations, partnerships, trusts, and individual proprietorships;
- Sensitive financial information contained within personal financial records of a judicial nomination candidate;
- Official background check of a judicial nomination candidate;
- Case reviews conducted by the Governor's Domestic Violence Fatality Review Board;
- Matters affecting an individual student, patient, or resident of a public institution;
- Preliminary discussions relating to acquisition (not sale) of real property;
- Security of a public body or agency, public building or facility, or the information system of a public body or agency, if open discussion would jeopardize security;
- Matters relating to information acquired and records of the Child Death Review Board;
- Matters relating to parimutuel racing;
- Matters relating to the care of children;
- Matters relating to patients and providers;
- Matters relating to maternity centers and child care facilities; and
- Matters relating to the Office of Inspector General.

Executive Session: Procedure

Requirements and restrictions on closed or executive sessions are contained in KSA 75-4319. Executive sessions are permitted only for the purposes specified. First, the public body must convene an open meeting and then recess into an executive session. Binding action may not be taken in executive session. Reaching a consensus in executive session is not in itself a violation of KOMA (*O'Hair v. United Sch. Dist. No. 300*, 15 Kan. App. 2d 52 (1991)). A "consensus," however, may constitute binding action and violate the law if a body fails to follow up with a formal open vote on a decision that normally would require a vote. The law does not require an executive session; the decision to hold an executive session is discretionary.

Generally, only the members of a public body may attend an executive session. The Attorney General indicates a public body may designate certain persons with essential information to assist in executive session deliberations. Inclusion of general observers means the meeting should be open to all members of the public.

Procedures for going into executive session include the following:

- Formal motion, seconded, and carried;
- Motion must contain a statement providing:
  - A statement describing the subjects to be discussed;
  - Justification for closure; and
  - Time and place open meeting will resume; and
- Executive session motions must be recorded in minutes. The law does not require other information to be recorded. Other minutes for open or executive sessions are discretionary, unless some other law requires them.

Compliance with KOMA during an Emergency Declaration

In March 2020, in response to the COVID-19 pandemic in Kansas, the State Rules and Regulation Board approved a temporary regulation proposed by the Attorney General to address compliance with KOMA during an emergency declaration. The regulation applies only during a state of disaster emergency or other emergency declaration lawfully declared (emergency), in the territory affected by the declaration, and to the extent emergency responses prevent or impede the ability of members of a body or agency subject to KOMA to meet by physically gathering in person or of members of the public to attend or observe public meetings by physically attending the meetings.

The regulation provides that all KOMA requirements remain in force and effect during an emergency, unless expressly suspended by order of the governor, as specifically outlined in the regulation.

The regulation specifies how a public body or agency may comply with KOMA's requirement that a meeting be "open to the public" by using a telephone or other medium for interactive communication, if the members of the body or agency are not gathering in person in a physical location to conduct the open meeting. These provisions include certain requirements related to technology, notice, and meeting procedure that must be met.

The regulation also contains similar provisions setting forth requirements that must be met to comply with KOMA if emergency responses prevent or impede the ability of the public to physically attend a public meeting occurring in person, and physical access of the public to the meeting place is limited.

Both the temporary regulation and a best practices document to aid in its implementation are available at *https://ag.ks.gov/open-government*. The Attorney General has announced his intent to seek permanent adoption of the temporary regulation.

Enforcement of KOMA

HB 2256 (L. 2015, ch. 68) changed enforcement of both KOMA and the Kansas Open Records Act (KORA). The law requires the Attorney General to provide and coordinate KOMA and KORA training throughout the state, including through coordination with appropriate organizations (KSA 75-761). Further, the statute gives the Attorney General or a county or district attorney various subpoena and examination powers in KOMA and KORA investigations (KSA 45-228; KSA 75-4320b).

Among other enforcement provisions, the bill allows the Attorney General or a county or district attorney to accept a consent judgment with respect to a KOMA or KORA violation, in lieu of filing an action in district court, and allows the Attorney General to enter into a consent order with a public agency or issue a finding of violation

to the public agency upon discovery of a KORA or KOMA violation (KSA 75-4320d; KSA 45-4320f).

HB 2290 (L. 2019, ch. 62) provides for repayment by a state agency to the Tort Claims Fund of the cost of defense or indemnification provided for the agency or employee arising out of an alleged violation of KOMA (KSA 75-6617).

Pursuant to KSA 75-753, the Attorney General compiles and publishes an annual report for each fiscal year with information about complaints and investigations involving KOMA and KORA. For fiscal year 2019, the Office of the Attorney General reported no complaints under KOMA against state agencies resulting in corrective action, two complaints against cities resulting in corrective action, six complaints against counties resulting in corrective action, and one complaint against a board of education resulting in corrective action. Additionally, 5 complaints were referred to county or district attorney offices, and 26 complaints resulted in a finding of no violation of KOMA.

For questions regarding application or suspected violations of KOMA, please contact the Office of the Attorney General. Limitations under Kansas law do not allow the Kansas Legislative Research Department to provide legal advice, interpretation of statute, or the legislative intent of a statute.

For more information, please contact:

Robert Gallimore, Managing Research Analyst
Robert.Gallimore@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

KLRD

Robert Gallimore
Managing Research Analyst
785-296-4420
Robert.Gallimore@klrd.ks.gov

Elections and Ethics

D-3 Kansas Open Records Act

Purpose

The Kansas Open Records Act (KORA) declares it is the public policy of Kansas that "public records shall be open for inspection by any person unless otherwise provided" (KSA 45-216). The burden of proving an exemption from disclosure is on the agency not disclosing the information (*SRS v. Public Employee Relations Board*, 249 Kan. 163 (1991)).

Who Is Covered by KORA?

KORA applies to those entities considered a "public agency" under the law (KSA 2019 Supp. 45-217).

Included in this definition are:

- The State;
- Any political or taxing subdivision of the State or any office, agency, or instrumentality thereof; and
- Any other entity receiving or expending and supported in whole or in part by public funds that are appropriated by the State or its political and taxing subdivisions.

The definition covers all state agencies, cities, counties, townships, school districts, and other special district governments, as well as any agencies or instrumentalities of these entities, and officers of the above public entities in connection with their official duties.

In addition, although not included in KORA itself, KSA 2019 Supp. 45-240 requires nonprofit entities, except health care providers, that receive public funds of at least $350 per year to adhere to certain open records requirements. The 2005 Legislature added this provision to require such nonprofit entities to document the receipt and expenditure of public funds and make this information available to the public. Like public agencies, nonprofit entities may charge a reasonable fee to provide this information.

Exclusions from Open Records Requirement

Certain entities and individuals are expressly excluded from the definition of "public agency" (KSA 2019 Supp. 45-217(f)(2)):

- Entities included only because they are property, goods, or services paid for with public funds;[1] and
- Any municipal, district, or appellate judge or justice.

What Is a Public Record?

"Public record" is defined broadly under KORA to mean "any recorded information, regardless of form, characteristics or location, which is made, maintained or kept by or is in the possession of any public agency; or . . . any officer or employee of a public agency pursuant to the officer's or employee's official duties and which is related to the functions, activities, programs or operations of any public agency" (KSA 2019 Supp. 45-217(g)(1)). Specifically excluded from the definition of "public record" are:

- Records owned by a private person or entity that are not related to functions, activities, programs, or operations funded by public funds, but "private person" shall not include an officer or employee of a public agency who is acting pursuant to the officer's or employee's official duties;
- Records kept by individual legislators or members of governing bodies of political and taxing subdivisions; or
- Employers' records related to certain individually identifiable employee records (KSA 2019 Supp. 45-217(g)(2) and (3)).

The Attorney General opined in 2015 (Op. Atty. Gen. 2015-010) that under certain specific conditions and the law in effect at the time, an email sent by a state employee from his or her private email account related to work funded by public funds is not within the meaning of public record. However, in 2016, the definition of and exclusions from "public record" were amended to broaden the definition of "public record" and apply it more specifically to state officers and employees, regardless of location of the record (KSA 2019 Supp. 45-217 (g)(1)). Additionally, audio and video recordings made and retained by law enforcement using a body camera or vehicle camera were added to the definition of a criminal investigation record (open only under specific circumstances) (KSA 2019 Supp. 45-254).

Right of Public to Inspect and Make or Obtain Copies of Records

All public records are open for inspection unless closed pursuant to specific legal authority (KSA 45-218(a) and (b)). Members of the public have the right to inspect public records during regular office hours and any established additional hours; the agency may require a written request but shall not require a request to be made in a particular form (KSA 2019 Supp. 45-220(a) and (b)). If the agency has business days on which it does not have regular office hours, it must establish reasonable hours when persons may inspect records and may not require a notice of desire to inspect more than 24 hours in advance of the hours established for inspection and obtaining copies; the agency also may not require the notice to be in writing (KSA 2019 Supp. 45-220(d)).

Any person may make abstracts or obtain copies of a public record. If copies cannot be made in the place where the records are kept, the records custodian must allow the use of other copying facilities (KSA 2019 Supp. 45-219(b)). Members of the public cannot remove a record without written permission of the custodian (KSA 45-218(a)).

KSA 2019 Supp. 75-3520 requires any document or record that contains any portion of an individual's Social Security number be redacted before it is made available for public inspection or copying. This does not apply to documents recorded in the official records of any county recorder of deeds or in the official records of the courts. An agency also is required to give notice, offer credit monitoring service at no cost, and provide certain information to individuals if

the agency becomes aware of the unauthorized disclosure of their personal information.

Digitalized information can meet the definition of a public record and must be provided in the form requested if the public agency has the capability of producing it in that form. The agency is not required to acquire or design a special program to produce information in a desired form, but it has discretion to allow an individual who requests such information to design or provide a computer program to obtain the information in the desired form (Op. Atty. Gen. 1988-152 [voter registration lists]; Op. Atty. Gen. 1989-106; and Op. Atty. Gen. 1987-137).

However, KORA explicitly states a public agency is not required to allow a person to obtain the electronic copies by attaching a personal device to the agency's computer equipment (KSA 2019 Supp. 45-219(g)).

A public agency is not required to provide copies of radio or recording tapes or discs, video tapes or films, pictures, slides, graphics, or illustrations unless the items were shown or played at a public meeting. Regardless, the agency is not required to provide items copyrighted by someone other than the public agency (KSA 2019 Supp. 45-219(a)).

Duties of Public Agencies

Under KORA, public agencies are required to:

- Appoint a freedom of information officer to assist the public with open records requests and disputes. That officer is to provide information on the open records law, including a brochure stating the public's basic rights under the law (KSA 45-226 and KSA 45-227);
- Adopt procedures to be followed to request and obtain documents (KSA 2018 Supp. 45-220(a));
- Respond to requests where it is possible to determine the records to which the requester desires access (KSA 2019 Supp. 45-220(b)); and
- Provide, upon request, office hours, name of custodian of record, fees, and procedures for obtaining records (KSA 2019 Supp. 45-220(f)).

Rights of Public Agencies

The public agency may:

- Require written certification the requester will not use names or addresses obtained from the records to solicit sales to those persons whose names or addresses are contained in the list (KSA 2019 Supp. 45-220(c));
- Deny access if the request places an unreasonable burden in producing the record or is intended to disrupt essential functions of the agency (KSA 45-218(e)); and
- Require payment of allowed fees in advance. Fees may include costs of any computer services and staff time, but may not exceed such costs (KSA 45-218(f); KSA 2019 Supp. 45-219(c)).

[*Note:* Executive Order 18-05 waives any charge or fee for the copying of documents, up to and including the first 100 pages, for all executive branch departments, agencies, boards, and commissions under the jurisdiction of the Office of the Governor in response to a KORA request made by any resident of Kansas.]

Prohibited Uses of Lists of Names and Addresses

With some specified exceptions, a list of names and addresses cannot be obtained from public records for the purpose of selling or offering for sale any property or service to the persons listed (KSA 2019 Supp. 45-220(c)(2) and KSA 2019 Supp. 45-230). This provision does not prohibit commercial use generally; it just applies to use of the names to sell or offer to sell property or a service. This provision does not prohibit the agency from using names and addresses in its public records for a purpose related to that

agency's services or programs (Op. Atty. Gen. 2006-026).

Any person, including the records custodian, who knowingly violates this provision of the law and gives or receives records for this purpose can be penalized with a civil fine not to exceed $500 in an action brought by the Attorney General or a county or district attorney (KSA 2019 Supp. 45-230).

Records That Must Be Closed

Some public records are required to be closed by federal law, state statute, or Supreme Court rule.

These types of public records must be closed and are broadly referenced in KSA 2019 Supp. 45-221(a)(1). Approximately 280 different statutes require closure of certain public records. A few examples include:

- Child in need of care records and reports, including certain juvenile intake and assessment reports (KSA 2019 Supp. 38-2209);
- Unexecuted search or arrest warrants (KSA 2019 Supp. 21-5906);
- Grand jury proceedings records (KSA 2019 Supp. 22-3012);
- Health care provider peer review records (KSA 2019 Supp. 65-4915(b)); and
- Certain records associated with the Kansas Department of Health and Environment's investigation of maternal death cases (KSA 2019 Supp. 65-177).

Records That May Be Closed

KSA 2019 Supp. 45-221(a)(1) to (55) lists other types of public records that are not required to be disclosed. The public agency has discretion to decide whether to make these types of records available. However, the burden of showing that a record fits within an exception rests with the party intending to prevent disclosure. The types of records that may be closed include:

- Records of a public agency with legislative powers, when the records pertain to proposed legislation or amendments. This exemption does not apply when such records are:
  - Publicly cited or identified in an open meeting or in an agenda of an open meeting; or
  - Distributed to a majority of a quorum of any body with the authority to take action or make recommendations to the public agency with regard to the matters to which these records pertain;
- Records of a public legislative agency, when the records pertain to research prepared for one or more members of the agency. Again, this exemption does not apply (*i.e.*, the records would be open) when such records are:
  - Publicly cited or identified in an open meeting or in an agenda of an open meeting; or
  - Distributed to a majority of a quorum of any body that has authority to take action or make recommendations to the public agency with regard to the matters to which such records pertain;
- Records that are privileged under the rules of evidence, unless the holder of the privilege consents to the disclosure;
- Medical, psychiatric, psychological, and alcohol or drug treatment records that pertain to identifiable individuals;
- Personnel records, performance ratings, or individually identifiable records pertaining to employees or applicants for employment in public agencies;
- Letters of reference or recommendation pertaining to the character or qualification of an identifiable individual and not related to the appointment of persons to fill a vacancy in an elected office;
- Information that would reveal the identity of any undercover agent or any informant reporting a specific violation of law;
- Criminal investigation records;

- Records of emergency or security information or procedures of a public agency; plans, drawings, specifications, or related information for any building or facility used for purposes requiring security measures in or around the building or facility; or for the generation or transmission of power, water, fuels, or communications, if disclosure would jeopardize security of the public agency, building, or facility;
- Attorney work product;
- Records of public agencies that identify home addresses of certain public officials such as judges, certain officers of the courts, and county and city attorneys; and
- Public records containing information of a personal nature when public disclosure would constitute a clearly unwarranted invasion of personal privacy.

Limited Disclosure Provisions

Some statutes provide for disclosure of limited information in response to KORA requests, rather than disclosure of the complete record requested.

Recently created limited disclosure provisions include those concerning body-worn and vehicle camera recordings and certain records of the Department for Children and Families (DCF) regarding child fatalities.

Body-worn and Vehicle Camera Recordings

Every audio or video recording made and retained by law enforcement using a body camera or vehicle camera must be considered a "criminal investigation record," as defined in KORA, thereby bringing such recordings within the exception to disclosure for criminal investigation records. This provision will expire July 21, 2021, unless reviewed and reenacted prior to that date (KSA 2019 Supp. 45-254).

In addition to any disclosures generally authorized for such recordings as criminal investigation records under KORA, the law allows certain persons to request to listen to an audio recording or to view a video recording. The law enforcement agency must allow access to these certain persons, within 20 days of the request, subject to a reasonable fee. The persons who may make such a request include the subject of the recording, any parent or legal guardian of a person under the age of 18 years who is a subject of the recording, an heir-at-law of a deceased subject of a recording, or an attorney for any of the previous persons listed (KSA 2019 Supp. 45-254(c)).

Child Fatality Information

House Sub. for SB 336 (L. 2018, ch. 87), among other provisions, added a requirement that the Secretary for Children and Families (Secretary), as allowed by applicable law, release within seven days the following information when child abuse or neglect results in a child fatality and a request is made under KORA: age and sex of the child; date of the fatality; a summary of any previous reports of abuse or neglect received by the Secretary involving the child, along with the findings of such reports; and any service recommended by DCF and provided to the child (KSA 2019 Supp. 38-2212(f)(3)).

The bill added a similar provision requiring the Secretary, as allowed by applicable law, to release the following information within seven days when a child fatality occurs while the child was in the custody of the Secretary and a request is made under KORA: age and sex of the child, date of the fatality, and a summary of the facts surrounding the death of the child (KSA 2019 Supp. 38-2212(f)(4)).

Sunset of Exceptions

A sunset provision for all exceptions added in 2000 required review of any exception within five years, or the exception would expire. It also required any exceptions continued after legislative review to be reviewed again five years later (KSA 2019 Supp. 45-229).

In 2013, the Legislature modified the review requirement in KSA 2019 Supp. 45-229 so that exceptions will no longer be subject to review and expiration if the Legislature has twice reviewed and continued the exemption or reviews and continues the exemption during the 2013 Session or thereafter (2013 HB 2012; L. 2013, ch. 50).

In 2020, Senate Sub. for HB 2137 (L. 2020, ch. 12) continued exemptions present in 10 statutes. Topics included, but were not limited to, law enforcement records identifying victims of certain crimes, public records identifying the home address of certain officials, treatment records in the possession of a treatment facility, and survey responses to audits conducted under the Legislative Post Audit Act.

Enforcement of the Open Records Law

HB 2256 (L. 2015, ch. 68) changed enforcement of both KORA and the Kansas Open Meetings Act (KOMA). The law requires the Attorney General to provide and coordinate KORA and KOMA training throughout the state, including through coordination with appropriate organizations (KSA 2019 Supp. 75-761). Further, the statute gives the Attorney General or a county or district attorney various subpoena and examination powers in KORA and KOMA investigations (KSA 2019 Supp. 45-228; KSA 2019 Supp. 75-4320b).

Among other enforcement provisions, the bill allows the Attorney General or a county or district attorney to accept a consent judgment with respect to a KORA or KOMA violation, in lieu of filing an action in district court, and allows the Attorney General to enter into a consent order with a public agency or issue a finding of violation to the public agency upon discovery of a KORA or KOMA violation (KSA 2019 Supp. 75-4320d; KSA 2019 Supp. 45-4320f).

Finally, HB 2290 (L. 2019, ch. 62) provides for repayment by a state agency to the Tort Claims Fund of the cost of defense or indemnification provided for the agency or employee arising out of an alleged violation of KORA (KSA 2019 Supp. 75-6617).

Pursuant to KSA 2019 Supp. 75-753, the Attorney General compiles and publishes an annual report for each fiscal year with information about complaints and investigations involving KORA and the Kansas Open Meetings Act. For FY 2019, the Attorney General's Office reported five complaints under KORA against state agencies resulting in corrective action, three complaints against cities resulting in corrective action, three complaints against counties resulting in corrective action, and two complaints against community colleges resulting in corrective action. Additionally, 3 complaints were referred to county or district attorney offices, and 29 complaints resulted in a finding of no violation of KORA.

For more information on KOMA, see article D-2 Kansas Open Meetings Act, available at *http://www.kslegresearch.org/KLRD-web/Briefing-Book-2021.html*.

Criminal Penalty for Altering Public Record

Altering, destroying, defacing, removing, or concealing any public record is a class A nonperson misdemeanor (KSA 2019 Supp. 21-5920).

For questions regarding application or suspected violations of KORA, please contact the Office of the Attorney General. Limitations under Kansas law do not allow the Kansas Legislative Research Department to provide legal advice, interpretation of statute, or the legislative intent of a statute.

1 See Ted Frederickson, *Letting the Sunshine In: An Analysis of the 1984 Kansas Open Records Act*, 33 Kan. L. Rev. 216-7. This analysis was utilized as recently as the 2017 Kansas Court of Appeals decision in *State v. Great Plains of Kiowa County, Inc.* (53 Kan. App. 2D 609, 389 P3d 984).

For more information, please contact:

Robert Gallimore, Managing Research Analyst
Robert.Gallimore@klrd.ks.gov

Natalie Nelson, Principal Research Analyst
Natalie.Nelson@klrd.ks.gov

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

KLRD

Matthew Willis
Research Analyst
785-296-4443
Matthew.Willis@klrd.ks.gov

Elections and Ethics

D-4 Voter Registration and Identification

Voter Registration and Requirements

National Voter Registration Requirements

Federal and state elections in the United States are generally run by the states themselves, according to Article I and Article II of the *U.S. Constitution*. Nevertheless, there are some federal requirements that impact voter registration in the states.

The Voting Rights Act of 1965 allows all U.S. citizens to vote at any election in any state, so long as they are otherwise qualified by law to vote in that election (42 USC §1971).

The National Voter Registration Act of 1993 (NVRA), also known as the "Motor Voter" law, expanded the locations where a person may register to vote by requiring states to allow driver's license applications to also serve as an application for voter registration.

The NVRA requires a voter registration application made as part of a driver's license application to include a statement containing each eligibility requirement (including citizenship) for that state (42 USC § 1993gg-3).

Finally, the Help America Vote Act (HAVA) (Public Law 107-252, § 303) requires applicants to provide one of the following when registering to vote:

- The applicant's driver's license number, if the person possesses a current and valid driver's license;
- The last four digits of the applicant's Social Security number, if the person does not possess a driver's license; or
- The applicant's state assigned identification number for voter registration purposes, for those applicants with neither a driver's license nor a Social Security number.

State Voter Registration Requirements

Every state except North Dakota requires voter registration. Generally, state voter registration laws require applicants to:

- Be 18 years old on or before the next election;
- Be a resident of the state where they are registering;
- Not be in jail and not have been convicted of a felony (or have had civil rights restored);
- Be mentally competent/not declared incapacitated; and
- Not be registered to vote in another state.

Same-day Voter Registration

Most states also have registration deadlines applicants must comply with to qualify to vote in an upcoming election. As of October 2020, 21 states and the District of Columbia have laws that allow same-day voter registration. Twenty of these states and the District of Columbia allow same-day registration on Election Day. One state (North Carolina) allows same-day registration only during the early voting period.

New Mexico passed legislation in the 2019 Legislative Session allowing qualified voters to register on Election Day beginning January 1, 2021.

During the 2019 Kansas Legislative Session, HB 2092, which would have enacted same-day voter registration in the state, was introduced and referred to the House Committee on Elections. The bill had a hearing and was worked by the Committee, but was not passed out for consideration by the full House of Representatives.

Online Voter Registration

As of October 2020, 41 states and the District of Columbia have laws allowing for online voter registration. Arizona was the first state to use online voter registration in 2002. Michigan, New Jersey, and North Carolina are the most recent states to adopt the practice. Michigan passed authorizing legislation in 2018, and New Jersey passed similar legislation in 2020. North Carolina did not require legislation to enact online voter registration. The states that have not provided for the use of online voter registration are Arkansas, Maine, Mississippi, Montana, New Hampshire, North Dakota (no registration required), South Dakota, Texas, and Wyoming.

Oklahoma is currently in the process of implementing phase two of the online voter registration passed in 2015. Starting in 2018, the state began allowing citizens to update their voter registration online. Phase two, which will allow new voter registrations online, was slated to be available by 2020 but appears to not be available yet.

Preregistration

The minimum age to vote in all federal and state elections is 18 years old. However, many states allow persons who are not yet 18 years old to register to vote before they turn 18 so they will be added to the voter rolls and able to vote as soon as they reach the required age. This practice is commonly referred to as preregistration and is administered by states in a variety of ways.

Twenty-six states allow an individual to register to vote if they will turn 18 on or before the next election, usually referring to the next general election. Fourteen states and the District of Columbia begin preregistration at 16 years of age, and 4 states allow such registrations beginning at 17 years of age. Five other states have their own unique age requirements: Alaska–90 days before 18th birthday; Georgia, Iowa, and Missouri–17 years, 6 months old; Texas–17 years, 10 months old.

North Dakota does not require voters to register, but specifies that qualified electors must be 18 years of age.

Automatic Voter Registration

The NVRA of 1993 required states to allow individuals to register to vote when applying for or renewing their driver's licenses. Some states

have taken this requirement a step further and adopted automatic voter registration (AVR).

AVR is a process by which individuals are automatically registered to vote and must opt out if they do not wish to be on the voter rolls. As of April 2020, 17 states and the District of Columbia have implemented AVR.

Voter Identification Requirements

As of August 2020, 36 states have enacted laws requiring or requesting voters to provide some form of identification (ID) before voting. However, there are many variations as to which forms of ID are accepted, whether the ID is required to include a photo, and what happens if a voter does not provide the required or requested ID upon arriving at the polling place.

North Carolina's voter ID statute is currently unenforceable under temporary injunctions issued in state court by the Court of Appeals of North Carolina and in federal court by the U.S. District Court for the Middle District of North Carolina. The Court of Appeals heard oral arguments in 2020 and are currently determining whether the statute is a form of voter suppression given past state actions and court rulings.

Kansas Law

Prior to the 2011 Legislative Session, Kansas law required persons voting for the first time in a county to provide ID unless they had done so when they registered. At that time, acceptable ID forms included a current, valid Kansas driver's license or nondriver's ID card, utility bill, bank statement, paycheck, government check, or other government document containing the voter's current name and address as indicated on the registration book. A voter's driver's license copy or number, nondriver's ID card copy or number, or the last four digits of the voter's Social Security number were acceptable when the voter was applying for an advance ballot to be transmitted by mail.

In 2011, the law changed significantly through the enactment of HB 2067. Effective January 1, 2012, all individuals voting in person were required to provide photo ID at every election (with the exception of certain voters, such as active duty military personnel absent from the country on Election Day), and all voters submitting advance ballots by mail were required to include the ID number on, or a copy of, a specified form of photo ID for every election. Free nondriver's ID cards and free Kansas birth certificates were available to anyone 17 or older for the purposes of meeting the new photo voter ID requirements. Each applicant for a free ID had to sign an affidavit stating he or she plans to vote and possesses no other acceptable ID form. The individual also had to provide evidence of being registered to vote.

Relatively minor amendments were also made in 2012 SB 129, including adding an ID card issued by a Native American tribe to the list of photo ID documents acceptable for proving a voter's identity when voting in person.

A U.S. District Court judge issued an order striking down Kansas' Voter ID law as it applies to registration for federal elections on June 18, 2018. (*Fish v. Kobach*, 309 F. Supp.3d 1048 (D. Kan. 2018).)

The decision was appealed to the U.S. Court of Appeals for the Tenth Circuit, which upheld the ruling of the U.S. District Court on April 29, 2020 (*Fish v. Schwab*, 957 F.3d 1105 (10th Cir. 2020)). On July 28, 2020, Secretary of State Scott Schwab petitioned for a writ of *certiorari* to the U.S. Supreme Court seeking to appeal the case.

For more information, please contact:

Matthew Willis, Research Analyst
Matthew.Willis@klrd.ks.gov

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

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

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