SCOTT SCHWAB
Secretary of State

Memorial Hall, 1st Floor
120 S.W. 10th Avenue
Topeka, KS 66612-1594
(785) 296-4564
sos.kansas.gov

STATE OF KANSAS

Testimony: SB454 (Proponent)
Senate Elections & Local Government Committee
Wednesday, March 11, 2020

Chairman Bowers and members of the Committee:

SB454 was introduced at the request of the Office of Secretary of State to add two exemptions for election security and cyber-security to the Kansas Open Records Act. As you will see from reviewing the bill, the exemptions are added to K.S.A. 45-221(a).

In Kansas, every record is subject to public release unless it is covered by an exemption. There are areas in state and federal law that are currently being used to cover election security and cyber-security. However, they are lacking in specificity and could subject the State to litigation. Our goal with SB424 is to provide a narrow exemption for material that is detailed enough it could be used by bad actors to penetrate our election systems.

Requests for election security records are becoming more frequent. Our office has not had an issue with any Kansas journalist on an open records request. In times where uncertainty exists on what they are seeking, we visit directly with the journalist to get more information and do our best to produce the records in a timely manner. The issue lies with out-of-state entities and national reporters who submit broad requests and question the specific authority we have to withhold any record. The provisions contained in SB424 provides clarity to state law to ensure we are not forced to produce details of system weakness or vulnerabilities, information that could be used to attack our systems, and specific defensive measures.

Since election infrastructure was reclassified as critical national infrastructure in 2017 (42 U.S.C 5192c), states throughout the nation have implemented provisions to account for election security and cyber-security. Some give very broad discretion to public officials while others include election or cyber threats under terrorism exemptions. Some even have very specific cyber-security provisions.

On Monday, our office met with the Kansas Broadcasters Association, Kansas Press Association, and the Sunshine Coalition to discuss SB454. We also reached out to the ACLU for their feedback on SB454. An agreement was quickly reached on revised language to ensure the bill does not unnecessarily limit access to information to the press or public. In summary, the language narrows the scope of the word “assessment” and folds election security into the definition of cyber-security. Our office is fully supportive of the attached language and want to thank the organizations for their help in improving the bill.

On behalf of the Office of Secretary of State, we respectfully ask for your support of SB454.

Respectfully submitted,

Clay Barker
Deputy Assistant Secretary of State
Assistant General Counsel

Attachment

BALLOON AMENDMENT to SB454

K.S.A. 45-217. As used in the open records act, unless the context otherwise requires:

***

(e) "Cybersecurity assessment" means an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.

(f) "Cybersecurity plan" includes, but is not limited to, information about a person's information systems, network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.

(g) "Cybersecurity vulnerability" means a deficiency within computer hardware or software, or within a computer network or information system, that could be exploited by unauthorized parties for use against an individual computer user or a computer network or information system.

***

K.S.A. 45-221. (a) Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose:

***

(12) Records of emergency or security information or procedures of a public agency *if disclosure would jeopardize public safety, including but not limited to records of cybersecurity plans, assessments, and vulnerabilities or procedures related to cybersecurity plans, assessments, and vulnerabilities*, or plans, drawings, specifications or related information for any building or facility which is used for purposes requiring security measures in or around the building or facility or which is used for the generation or transmission of power, water, fuels or communications, if disclosure would jeopardize security of the public agency, building or facility.