KANSAS OFFICE of
REVISOR of STATUTES
LEGISLATURE of THE STATE of KANSAS
Legislative Attorneys transforming ideas into legislation.

300 SW TENTH AVENUE ▪ SUITE 24-E ▪ TOPEKA, KS 66612 ▪ (785) 296-2321

MEMORANDUM

To: Chairwoman McGinn and members of the Senate Ways and Means Committee

From: Jill Wolters, First Assistant Revisor, and Jenna Moyer, Assistant Revisor

Date: February 1, 2018

Subject: **SB342 – Enacting the Kansas cybersecurity act.**

SB342 creates the Kansas information security office, chief information security officer, and establishes the cybersecurity state fund. HB2560 is an identical bill in the House.

Section 1 – States the name of the act and the sections of the bill that the act applies to.

Section 2 – Defines common terms used in the bill.

Section 3 – Establishes the position of the executive branch chief information security officer (CISO), appointed by the governor, and the duties of this position. These duties include:

- serving as the executive branch chief cybersecurity strategist;
- overseeing cybersecurity training for executive branch agencies;
- ensuring technology resources provided to governmental entities comply with applicable laws and rules and regulations;
- coordinating cybersecurity efforts among governmental entities and private vendors;
- approving executive branch agency cybersecurity plans for information technology (IT) projects;
- halting executive branch agency IT projects that are not compliant with approved cybersecurity plans;
- conducting security assessments of executive branch agency IT systems;
- the authority to suspend public access to executive branch agency IT resources when the compromise of personal information has occurred or is likely to occur; and
- hiring/promoting/disciplining/dismissing all executive branch cybersecurity positions.

Section 4 – Establishes the Kansas information security office (KISO) and the duties of the office. The KISO is considered a separate state agency for the purposes of the budget. The KISO duties include:

- assisting executive branch agencies to develop and implement information security risk-management programs;
- providing executive branch agencies strategic risk guidance;
- creating and managing a unified/flexible control framework to integrate/normalize requirements resulting from global laws/standards/regulations;

- ensuring security programs and technology from state vendors comply with relevant laws and rules and regulations;
- managing frameworks to measure effectiveness of state information security programs;
- coordinating the use of external information security resources involved in IT security programs;
- helping develop policies and plans for disaster recovery and cybersecurity events; and
- coordinating IT security among governmental entities at the state and local levels.

Section 5 – Sets out duties for heads of governmental entities that connect to state network resources. These include:

- being solely responsible for all data and IT resources of the governmental entity;
- ensuring the entity has an information security program in place;
- implementing policies to ensure such entity's data and resources are maintained in compliance with applicable federal and state law and rules and regulations;
- implementing safeguards to reduce, eliminate or recover from threats to IT and data;
- attending annual entity head cybersecurity training;
- preparing a cybersecurity report every two years to the CISO that identifies vulnerabilities, in addition to an annual internal assessment of the security program; and
- complying with notification requirements in the event of a breach.

Section 6 – All governmental and non-governmental entities connecting to state network resources shall demonstrate cybersecurity effectiveness as provided in this section. If the CISO determines that an entity is unable to meet compliance standards, the entity shall be disconnected from state network resources, unless the CISO determines that the entity is working in good faith to comply.

Section 7 – Requires governmental entities that process personal information on their websites or applications to establish policies to protect the confidentiality of that information.

Section 8 – Authorizes the CISO to require governmental entities and their contractors who work with personal information to be fingerprinted and submit to a criminal history record check at least every five years.

Section 9 – Categorizes information security plans and reports as confidential, exempting this information from open records law.

Section 10 – Establishes the cybersecurity state fund and how moneys in this fund can be used by the KISO.

Section 11 – Authorizes the KISO to enter into multiple-year leases and acquisition contracts subject to appropriation acts.

Section 12 – Gives the CISO authority to adopt rules and regulations. These include the establishment of rates for services provided to governmental entities and establishing a base rate per employee for all governmental and non-governmental entities connecting to state resources. This rate shall not exceed $700 per employee per year and its adequacy will be assessed by the government, technology and security committee every two years beginning in 2022.

Section 13 – Authorizes the KISO to provide cybersecurity services and charge for services that are furnished to governmental entities. Collection of the payments authorized by this act start on July 1, 2020.

Section 14 – Establishes how governmental entities can pay for cybersecurity services.