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: House Committee on Government, Technology and Security

From: Jenna Moyer, Assistant Revisor of Statutes

Date: January 31, 2018

Subject: HB2560 – Enacting the Kansas cybersecurity act.

HB2560 creates the Kansas information security office, chief information security officer, and establishes the cybersecurity state fund.

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 chief information security officer (CISO) and the duties of this position. These duties include:

- Assist executive branch agencies to develop and carry out information security programs;
- provide executive branch agencies guidance on IT projects;
- oversee cybersecurity training for executive branch agencies
- ensure state vendors comply with relevant laws and rules and regulations; and
- help to develop disaster and recovery policies and to coordinate IT security interests between different levels of government

Section 4 – Establishes the Kansas information security office (KISO) and the duties of the office. These duties include:

- Assist executive branch agencies to develop and implement information security risk-management programs;
- ensure security programs and technology from state vendors comply with relevant laws and rules and regulations;
- manage framework to measure effectiveness of state information security programs
- coordinate use of external information security resources with contract negotiation
- help develop policies and plans for disaster recovery and cybersecurity events
- coordinate information technology security among governmental entities at the state and local levels

Attachment 1
GTS 1-31-18

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

- Being solely responsible for all of the entity's data and IT resources;
- ensuring the entity has an information security program in place;
- implement safeguards to reduce, eliminate or recover from threats to IT and data;
- attend annual entity head cybersecurity training;
- preparing a cybersecurity report to the CISO that identifies vulnerabilities; and
- comply with notification requirements in the event of a breach.

Section 6 – Sets out requirements for governmental and non-governmental entities to connect to state network resources.

Section 7 – Requires governmental entities to establish policies to protect the confidentiality of personal information that may be processed on an internet website or mobile application.

Section 8 – Authorizes the CISO to require employees or contractors of governmental entities who work with personal information to be subject to fingerprinting and criminal history record checks 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.

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.

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