

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: Senate Ways and Means
From: Jenna Moyer, Assistant Revisor of Statutes
Date: March 13, 2018
Subject: Sub for HB 2359 – Enacting the Kansas cybersecurity act for executive branch agencies.

Substitute for HB 2359 creates the Kansas information security office and the position of chief information security officer.

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.

One definition to note is “executive branch agency”, which excludes elected office agencies (*i.e.* attorney general, secretary of state), KPERs, the board of regents and board of regents’ institutions.

Section 3 – Establishes the position of chief information security officer (CISO) and the duties of this position. These duties include:

- Serving as the executive branch cybersecurity strategist and authority;
- Ensuring resources provided to executive branch agencies comply with applicable laws and regulations;
- Coordinating cybersecurity efforts between executive branch agencies; and
- Providing guidance to executive branch agencies relating to an identified high-risk vulnerability or threat.

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

- Assisting executive branch agencies to develop and implement information security risk-management programs;
- Using ITEC developed standards, create and manage a control framework to integrate and normalize legal requirements;
- Providing strategic risk guidance for executive branch IT projects;
- Coordinating the use of external resources in information security programs;
- Helping develop policies and plans for disaster recovery and cybersecurity events;

- Ensuring cybersecurity training is provided to executive branch agencies; and
- Providing an annual status report of executive branch cybersecurity programs to the Joint Committee on Information Technology and the House Government, Technology and Security Committee.

Section 5 – Sets out the duties for executive branch agency heads, which include:

- Being solely responsible for all of the agency’s data and IT resources;
- Ensuring the agency has an information security program in place;
- Implementing policies to ensure the agency’s data and IT resources comply with applicable laws and regulations
- Implementing safeguards to reduce, eliminate or recover from threats to IT and data;
- Preparing a cybersecurity report to the CISO that identifies vulnerabilities;
- Attend annual agency leadership training; and
- Comply with notification requirements in the event of a breach.

Section 6 – Authorizes executive branch agency heads to require their employees and contractors who work with personal information to be fingerprinted and submit to a criminal history record check at least every five years.

Section 7 – Categorizes information collected pursuant to this act as confidential, unless data elements and information that would place the organization at risk have been redacted.

Section 8 – Establishes that executive branch agencies can pay for cybersecurity services through existing budgets, grants or other revenues, or through a special assessment.