STATE OF KANSAS

CORPORATION COMMISSION
1500 SW ARROWHEAD ROAD
TOPEKA, KS 66604-4027

PHONE: 785-271-3100
FAX: 785-271-3354
http://kcc.ks.gov/

GOVERNOR JEFF COLYER, M.D.
SHARI FEIST ALBRECHT, CHAIR | JAY SCOTT EMLER, COMMISSIONER | PAT APPLE, COMMISSIONER

Before Senate Ways and Means
March 13, 2018

Neutral Testimony (Written)
On Substitute HB 2331 and Substitute HB 2359

Submitted by Jon McKenzie, IT Security Analyst
On Behalf of the Staff of the Kansas Corporation Commission

Chair McGinn, Vice Chair Billinger, Ranking Minority Member Kelly, and members of the committee.

We all agree cybersecurity should be a priority and the Kansas Corporation Commission (KCC) has been proactive and made IT security a priority. The KCC understands that not all agencies have the resources to focus on cybersecurity and efforts should be made to improve the cybersecurity of the state's information technology system. However, the process and controls to improve security should not be rushed. The needs of the agencies, the State and OITS' ability to meet those needs should be evaluated and understood. These bills create more concerns and questions than they address or resolve.

Both bills are extremely abstract and heavy on reports/policies/regulations, but little or no mention of preventative action on behalf of the CISO/OITS to assist agencies in reducing their security issues.

- What does OITS/CISO do to act upon security vulnerabilities today? At the KCC we see critical threats getting to our firewalls even though our traffic has already traversed the OITS/CISO security perimeter.
- Both bills create a security bureaucracy that is heavy on policy/reports with no definite ACTION priorities/goals.
- How is security improved? Policy/procedures are nice, but what actions will be taken to improve security?
- Will the reports be reviewed by qualified staff and acted upon? Or will they simply be a checkbox that the agency submitted the report?
- Neither bill addresses how OITS/CISO will assist agencies to improve their security profile other than reports/policies.

Why should KCC be different from "elected office agencies, Kansas public employees retirement system or regents' institutions"? The KCC has a robust security program in place and should be added to the exempt agencies.

Security is a team effort. IT decisions/actions are important. Management support/actions are important. It is important that agency staff and management know the IT staff and feel comfortable reporting issues and that those issue are acted upon timely and appropriately. In a consolidated environment that relationship does not exist and it is an important component of security. This is analogous to a trusted neighbor looking after your house while you are away on vacation. That simple personal relationship can prevent many issues.

Substitute HB 2331 would provide for the creation of the Kansas Information Security office and centralize cybersecurity for all executive branch agencies. This bill would further create the Kansas Information Technology Enterprise (KITE) and consolidate information technology administration for all executive branch agencies.

Starting small and developing a viable program should be considered. It would be much better to merge the IT/security staff of a few small agencies into a larger agency that already has a strong security profile, take action to improve the security as a whole. This process could then be repeated annually or bi-annually resulting in the security profile of entire state government improving with time. The implosion of all agencies' IT into OITS could have many unintended consequences.

Substitute HB 2359 does little that does not exist today, with the exception of an added burden on agencies to provide reports to the CISO.

OITS already maintains the state network firewalls and related security environment. If OITS is reviewing the logs/reports from those systems they may be able to prevent vulnerabilities before that network traffic gets to the agencies' security equipment.

Section 5 puts the burden on the agency heads, just as it exists today. The bulk of this bill leaves the security responsibilities at the agency level, resulting in a CISO bureaucracy above the agency.

Section 5 (h)(1) requires the submission of an annual assessment report of just about any connected device including software and even contractors. How is an agency supposed to evaluate the extent of any exposure for Microsoft, Apple, Dell, Oracle? Some of the largest software/hardware companies in the world? Agencies simply do not have the expertise to do this. Nor do outside contractors that an agency could afford to hire in Kansas. About all an agency could do is to re-publish the monthly/quarterly vulnerability/ patch list provided by these large vendors and state that the agency made every attempt to implement the patches as recommended. Additionally, a "point in time" report of the extent of exposure is like asking "what are your chances of getting the flu"? There are simply too many dependencies/variations for an annual report.

Section 5 (h)(2) requires annual internal assessments of its security program and those assessments are confidential, until July, 1, 2023. If the Legislature does not act, do those assessments become publically available?

Section 5 (h)(3) indicates we need to prepare a summary of the above and provide it to the public on request. What would an agency put in this summary that would be of value to the public? Security information is exempt under the Kansas Open Records Act (KORA).

Section 7. KORA already exempts security as confidential, so this section is redundant with current law.