SCOTT SCHWAB
Secretary of State

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

STATE OF KANSAS

March 15, 2024

Testimony on HB2842 (In Person / Neutral)
House Committee on Legislative Modernization
Monday, March 18, 2024

Chair Wasinger and members of the Committee:

Thank you for the opportunity to provide testimony on House Bill 2842. The Secretary of State's Office supports the effort to strengthen the state's cybersecurity. The office, however, wishes to provide the following observations about certain provisions in the bill and the agency's cybersecurity activities.

In 2017, elections were designated as critical infrastructure by the federal government. As a result, among other things, for the last seven years the office has worked closely with CISA and other state and federal security partners on a regular basis, conducting routine risk assessments and testing, and has robust cybersecurity measures in place. The agency already meets certain requirements in the bill. For example, for the past five years, the agency has required all staff to complete annual cybersecurity awareness training, in addition to periodic cybersecurity training and testing throughout the year. In addition, we currently have an agreement with Kansas Information Security Office (KISO) to administer our boundary firewalls and we frequently submit suspicious activity to be analyzed.

In addition, the Kansas Secretary of State's website (sos.ks.gov) was already moved to a .gov address as a means of heightening security and providing confidence to users that they are reaching a secure government website. Related websites are in the process of being transitioned to a .gov extension which will be completed before August 2024. It was unclear if the .gov requirement applies to counties or other subdivisions of government.

With respect to specific sections of the bill, the agency notes the following:

Section 1: It is unclear whether statewide elected officials are included in Section 1, which requires all information technology services, including cybersecurity services, for each branch of state government to be administered by the chief information technology officer (CITO) and the chief information security officer (CISO) of such branch. It appears that Section 1 may conflict with Section 15 which requires the CITO to review and consult with executive branch agencies on technology plans and monitor agency compliance with information technology resource policies and procedures. It is unclear whether agencies would maintain their dedicated IT staff when

reviewing these provisions together. The agency has significant concerns about any proposal that would shift IT staff out of the agency and the security risk this could pose to the elections system.

Section 1 also provides that beginning July 1, 2025, funds appropriated from the state general fund to or any special revenue fund of any state agency for information technology and cybersecurity expenditures shall be appropriated as a separate line item. The agency notes concern about the potential detail of information that may be required to be provided and potential security risk of disclosing confidential information.

We are uncertain of the definition depth of "integrate ". Would this mean placing restrictions on future agency purchases and software development?

Section 11: The agency currently has staff who perform the work of a chief information security officer (CISO) but is not titled as such. Is the bill's intent to require a dedicated staff member to fill this role? Such a requirement would require approval for an additional FTE and funding for salary and benefits.

The bill requires agencies to develop a cybersecurity program for the office that complies with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. The requirements of CSF 2.0 have not yet been fully vetted by the agency to determine if additional costs or personnel are required to achieve compliance. The agency also has concerns about referencing a specific version of CSF in the law which could become outdated as newer versions are released. Further, it is unclear how the NIST score is determined.

Finally, Section 11 requires the agency to coordinate with CISA to perform annual audits of the office for compliance with applicable state and federal laws, rules and regulations and office policies and standards. The agency notes that while CISA provides process audits against industry standards, it does not provide audits against state law or regulation.

Thank you for the opportunity to testify.

/*Clayton Barker*

Clayton L. Barker
Deputy Secretary of State, General Counsel
Office of the Kansas Secretary of State
clay.barker2@ks.gov