SUBJECT: Revising statute governing state and local government information security

COMMITTEE: State Affairs — favorable, without amendment

VOTE: 13 ayes — Hunter, Hernandez, Anchía, Dean, Geren, Guillen, Metcalf, Raymond, Slawson, Smithee, Spiller, S. Thompson, Turner

0 nays

SENATE VOTE: On final passage (April 17) — 31 - 0

WITNESSES: None *(considered in a formal meeting on May 12)*

BACKGROUND: Some have suggested that updating provisions related to the state's information technology planning and tools could improve the cybersecurity of state agencies and facilitate better resource sharing.

DIGEST: SB 1204 would revise provisions governing the sharing of information resources between state agencies and with the Department of Information Resources (DIR).

State agency information security assessment. The bill would remove the inclusion of a state agency's data governance program in the agency's information security assessment required to be conducted every two years. The bill would require each state agency to complete the information security assessment in consultation with DIR or the DIR-selected vendor and submit the results of the assessment to DIR.

The bill would remove provisions requiring DIR to establish the requirements for the assessment. The bill also would repeal provisions requiring an agency to report the results of the information security assessment to DIR and to other entities on request.

State agency information technology infrastructure. As part of DIR's collection of information on the status and condition of each state agency's information technology infrastructure, DIR would be required to collect

the results of the information security assessment. Rather than providing the information to DIR according to a schedule that DIR determined, each state agency would be required to provide the information by June 1 of each even-numbered year.

The bill would require DIR to assign to each state agency, other than an institution of higher education, an information security rating of average, above average, or below average based on the agency's information security risk profile. In assigning this rating, DIR would consider:

- the information the agency provided regarding the status and condition of the agency's information technology infrastructure;
- the agency's comprehensive information security risk position relative to the agency's risk environment; and
- any additional document or information DIR requested.

DIR would be required to develop options and make recommendations for improvements in the information security maturity of any state agency assigned an information security rating of below average. DIR could assist any state agency in determining whether additional security measures would increase the agency's information security maturity.

DIR could audit the information security and technology of any state agency assigned an information security rating or contract with a vendor to perform the audit. DIR would have to make the results of an audit available on request of the governor, chair of the House appropriations committee, chair of the Senate finance committee, speaker of the House of Representatives, lieutenant governor, and staff of the Legislative Budget Board (LBB).

In addition to submitting a consolidated report of the information submitted by state agencies to the above entities, DIR would need to submit to those entities any DIR recommendations relevant to and necessary for improving the state's information technology infrastructure and information security.

The bill would repeal provisions classifying the consolidated report as public information and requiring the report to be released or made available to the public on request, with certain exceptions. The bill would require DIR to compile a summary of the consolidated report and make the summary available to the public. The summary could not disclose any confidential information. The consolidated report and all information a state agency submitted to substantiate or otherwise related to the report would be confidential and not subject to disclosure. The state agency or DIR could redact or withhold information as confidential without requesting a decision from the attorney general.

Following review of the consolidated report, LBB could direct DIR to select for participation in a statewide technology center any state agency assigned an information security rating. The bill would require DIR to notify each selected state agency of its selection. DIR would not be required to conduct a cost and requirements analysis for a selected state agency. These provisions would expire September 1, 2027.

Information sharing and analysis organization. The bill would specify that DIR's current information sharing and analysis organization was an intrastate organization. The bill also would authorize DIR to establish an interstate information sharing and analysis organization to provide a forum for states to share information regarding cybersecurity threats, best practices, and remediation strategies.

Digital signatures. The bill would specify that, unless expressly prohibited by other law or a rule adopted by the state agency, a state agency would be required to accept a digital signature included in any communication or payment electronically delivered to the state agency.

Designated information security officer. An information security officer designated by each state agency could serve as a joint information security officer by two or more state agencies. DIR would have to approve the joint designation.

Technology improvement and modernization fund. The bill would

allow money in the technology improvement and modernization fund to be used to mitigate a breach or suspected breach of system security or the introduction of ransomware into a computer, computer network, or computer system at a state agency. Money in the fund could not be used to pay a person who committed the offense of electronic data tampering.

Guidance on use of distributed ledger technology. DIR would be required to develop and disseminate guidance for the use of distributed ledger technology, including blockchain, among state agencies. The guidance would need to include a framework or model for deciding if distributed ledger technology was appropriate for meeting a state agency's needs. The guidance could include examples of potential uses of distributed ledger technology by an agency, sample procurement and contractual language, and information on educational resources for agencies on distributed ledger technology. DIR would be required to develop and disseminate the guidance and decision model by December 1, 2023.

Peer-to-peer payment systems. The bill would allow a state agency or local government that used the state electronic Internet portal to use peer-to-peer payments for point-of-sale, telephone, and mail transactions. DIR would be required to identify at least three commonly used peer-to-peer payment systems that provided for data privacy and financial security and post a list containing those systems in a conspicuous location on its website. The bill would require DIR to biennially review and update the list as necessary. The bill would define "peer-to-peer payment system" as a digital non-credit card system used for transferring funds from one party to another.

Marketing of services. The bill would authorize DIR to use appropriated money to market to state agencies and local governments shared information resources technology services offered by DIR, including data center services, disaster recovery services, and cybersecurity services. Such an expenditure would have to be approved by the executive director.

State agency strategic plans. Except as otherwise modified by the

Legislative Budget Board or the governor, DIR-prepared instructions would have to require each state agency's strategic plan to include a description of customer service technology, including telephone systems and websites, that improved customer service performance.

Information technology modernization plan. As part of each state agency's strategic plan, a state agency would have to include an information technology modernization plan that outlined the manner in which the agency intended to transition its information technology and data-related services and capabilities into a more modern, integrated, secure, and effective technological environment. DIR could provide a template for the information technology modernization plan.

The bill would take effect September 1, 2023.