SUBJECT: Revising state agency information resources cybersecurity requirements

COMMITTEE: State Affairs — favorable, without amendment

VOTE: 12 ayes — Phelan, Hernandez, Deshotel, Guerra, Harless, Holland, Hunter, P. King, Parker, E. Rodriguez, Smithee, Springer

0 nays

1 absent — Raymond

SENATE VOTE: On final passage, April 26 — 30-0, on Local and Uncontested Calendar

WITNESSES: For — (*Registered, but did not testify*: Leticia Van de Putte, City of Del Rio and San Antonio Chamber of Commerce; Tom Nobis)

Against — None

On — (*Registered, but did not testify*: Nancy Rainosek, Department of Information Resources)

BACKGROUND: In interim hearings held by the Senate Select Committee on Cybersecurity, some suggested several updates to statutory provisions governing cybersecurity policies to better protect state agency data and ensure that key services were delivered adequately.

DIGEST: SB 64 would revise various cybersecurity requirements for state agency information resources, including oversight of cybersecurity practices and the state's electric grid.

Information sharing and analysis organization. The bill would rename the current information sharing and analysis center, which provides a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies, as the information sharing and analysis organization. The bill would expand participation in the organization to include local governments, public and private

institutions of higher education, and the private sector.

A participant would have to assert any exception available under state or federal law in response to a request for public disclosure of information shared through the organization. Statute allowing a governmental body to voluntarily make available information to the public would not apply to the shared information.

The Department of Information Resources (DIR) no longer would be required to appoint representatives from state agencies or use funds other than those appropriated in the general appropriations act for the organization.

Information security plan. SB 64 would require each state agency to include in its information security plan required under state law a written document that was signed by the head of the agency, the chief financial officer, and each executive manager and stated that those persons had been made aware of the risks revealed during the preparation of the plan.

Information technology infrastructure report. The bill would revise the requirements for the biennial report that DIR has to submit to certain persons on the condition of state agencies' information technology infrastructure. For a state agency found to be at higher security and operational risk, the report would have to include a detailed analysis of agency efforts to address the risks and related vulnerabilities, and for such an agency, the report no longer would have to include an estimate of the costs to address the risks and vulnerabilities through certain activities.

Cybersecurity report. SB 64 would revise the requirements for a biennial report DIR is required to submit identifying preventive and recovery efforts the state can undertake to improve state cybersecurity. Under the bill, the report would have to evaluate a program that provided an information security officer to assist small agencies and local governments that were unable to justify hiring a full-time information security officer. The report no longer would have to evaluate the costs and benefits of cybersecurity insurance or tertiary disaster recovery options.

Vulnerability reports. The bill would require the information security officer of a state agency, instead of its information resources manager, to prepare a report on the vulnerability of a computer network, system, program, software, or other device to unauthorized access or harm. The security officer would provide an electronic copy of the report to the agency's information resources manager.

Prioritized projects report. By October 1 of each even-numbered year, DIR would have to submit a report to the Legislative Budget Board that prioritized, for the purpose of receiving funding, state agency cybersecurity and legacy system replacement or modernization projects. Each state agency would have to coordinate with DIR to implement this requirement.

A state agency would have to assert any exception available under state or federal law in response to a request for public disclosure of information contained in or written, produced, collected, assembled, or maintained in connection with the report. Statute allowing a governmental body to voluntarily make available information to the public would not apply to the report.

Security breach notification. The bill would require a state agency that owned, licensed, or maintained computerized data that included sensitive personal or confidential information to notify DIR, including the chief information security officer, of the details of a breach, suspected breach , or unauthorized exposure within 10 business days after eradication, closure, and recovery. The notification would have to include an analysis of the event's cause.

The agency no longer would have to notify the state cybersecurity coordinator within 48 hours of the discovery of the event, while other notification requirements under current law would remain.

Investigating cybersecurity event. The review and analysis of computer-based data for the purpose of preparing for or responding to a

cybersecurity event would not constitute an investigation for the purposes of provisions governing investigations companies and would not require licensing under the Private Security Act.

Cybersecurity degree programs. SB 64 would require the Texas Higher Education Coordinating Board, in collaboration with DIR, to identify strategies to incentivize institutions of higher education to develop cybersecurity degree programs. By September 1, 2020, the coordinating board would have to report the strategies to the lieutenant governor, House speaker, certain legislative committees, and each governing board of an institution of higher education.

Cybersecurity program for utilities. The bill would require the Public Utility Commission (PUC) to establish a program to monitor cybersecurity efforts among utilities in Texas. For the purposes of this requirement, the bill would define "utility" as an electric cooperative, an electric utility, a municipally owned electric utility, a retail electric provider, or a transmission and distribution utility.

The program would have to provide guidance on best practices in cybersecurity and facilitate the sharing of cybersecurity information between utilities. It also would have to provide guidance on best practices for cybersecurity controls for supply chain risk management of cybersecurity systems used by utilities, which could include those related to software integrity and authenticity, vendor risk management and procurement controls, and vendor remote access.

PUC could collaborate with the state cybersecurity coordinator and the cybersecurity council in implementing the program.

ERCOT cybersecurity assessment. The bill would require the Electric Reliability Council of Texas (ERCOT) to conduct an internal cybersecurity risk assessment, vulnerability testing, and employee training to the extent the activities were not otherwise required under applicable state and federal laws.

ERCOT also would have to submit an annual report to the PUC on compliance with applicable cybersecurity and information security laws. Information in the report would be confidential and not subject to disclosure under public information laws.

Disaster definition. The bill would add a cybersecurity event to the list of occurrences or imminent threats that were considered a disaster for the purposes of the Texas Disaster Act.

Retirement systems. The bill would require the Employees Retirement System of Texas and the Teacher Retirement System of Texas to comply with laws governing cybersecurity and information security standards established by DIR.

Public junior colleges. The bill would apply laws governing information resources to public junior colleges as necessary to comply with information security standards for participation in shared technology services and statewide technology centers. DIR by agreement could provide network security to a public junior college.

Other provisions. The bill would repeal provisions governing bids or proposals for interagency contracts for information resources technologies and data security procedures for online and mobile applications of institutions of higher education.

To the extent of any conflict, SB 64 would prevail over another bill of the 86th Legislature relating to non-substantive additions to and corrections in enacted codes.

Effective date. The bill would take effect September 1, 2019.