SUBJECT: Establishing certain information management and security programs

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 13 ayes — Paddie, Hernandez, Deshotel, Harless, Howard, Hunter, P. King, Lucio, Metcalf, Raymond, Shaheen, Slawson, Smithee

0 nays

SENATE VOTE: On final passage, April 19 — 31-0, on Local and Uncontested Calendar

WITNESSES: For — Hope Osborn, Texas 2036; (*Registered, but did not testify*: Jason Winborn, AT&T; James Hines, Internet Association; Myra Leo, Methodist Healthcare Ministries; Nora Belcher, Texas e-Health Alliance; Travis Broussard, UiPath)

Against — None

On — (*Registered, but did not testify*: Amanda Crawford, Ed Kelly, and Nancy Rainosek, Texas Department of Information Resources; Jordon Dixon, Health and Human Services Commission)

BACKGROUND: The Texas Cybersecurity Council and the Texas Privacy Protection Advisory Council have made recommendations to improve cybersecurity standards and data management practices for state agencies and local governments, and it has been advised that these recommendations be implemented in statute.

DIGEST: CSSB 475 would require the Texas Department of Information Resources (DIR) to establish a state risk and authorization management program and to establish the Texas Volunteer Incident Response Team. DIR also would have to appoint a data management advisory committee and establish a framework for regional cybersecurity working groups, and would be authorized to establish regional network security centers. The bill also would implement requirements for certain state agency contracts, prohibit the collection or dissemination of certain individually identifying

information, and require state agencies to appoint data management officers, among other provisions.

State risk and authorization management program. CSSB 475 would require DIR by December 1, 2021, to establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that processed state agency data. DIR by rule would have to prescribe the categories and characteristics of cloud computing services subject to the program and the requirements for vendor certification.

The program would have to allow a vendor to demonstrate compliance by submitting documentation showing the vendor's compliance with a risk and authorization management program of the federal government or another state that DIR approved.

State agencies would have to require vendors with whom they contracted to provide cloud computing services to comply with the program's requirements throughout the term of the contract. DIR would be required to evaluate vendors to determine whether a vendor qualified for certification issued by the department reflecting compliance with program requirements.

Agencies would have to ensure that each contract for cloud computing services they entered into or renewed on or after January 1, 2022, complied with the program.

Volunteer incident response team. CSSB 475 would require DIR to establish the Texas Volunteer Incident Response Team to provide rapid assistance to participating entities during cybersecurity events. "Participating entities" would include state agencies, including institutions of higher education, or local governments that received assistance during a cybersecurity event.

DIR would have to establish the team by December 1, 2021.

Volunteer eligibility, contract. DIR would have to prescribe eligibility criteria for participation as a volunteer member of the incident response team, including a requirement that each volunteer have expertise in addressing cybersecurity events. The department also would have to enter into a contract with each volunteer that required the volunteer to:

- acknowledge the confidentiality of certain information;
- protect all confidential information from disclosure;
- avoid conflicts of interest that might arise in deployment as part of the incident response team;
- comply with DIR security policies and procedures;
- consent to background screening required by DIR; and
- attest to the volunteer's satisfaction of any established eligibility criteria.

DIR would have to require criminal history record information for each volunteer and could request other information relevant to the volunteer's qualifications.

Deployment. In response to a cybersecurity event that affected multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, and on request of a participating entity, DIR could deploy volunteers and provide rapid response assistance under its direction and the managed security services framework established by statute to assist with the event. Volunteers could only accept deployment in writing and could decline to accept a deployment for any reason.

DIR powers and duties. The bill would require DIR to:

- approve the incident response tools the incident response team could use in responding to a cybersecurity event;
- establish volunteer eligibility criteria;
- develop and publish guidelines for operation of the incident response team; and

- adopt rules necessary to implement the establishment of the response team.

DIR could require participating agencies to enter a contract as a condition for obtaining assistance from the incident response team, and such contracts would have to comply with certain statutory requirements.

The department also could provide training to volunteers, use available money to compensate volunteers for deployment expenses, and establish a fee schedule for participating agencies receiving response team assistance. The amount of fees collected could not exceed the costs of operating the response team.

Cybersecurity council duties. The cybersecurity council would have to review and make recommendations to DIR regarding policies and procedures used by the department to implement the bill's provisions related to the volunteer incident response team, and DIR could consult with the council in implementing and administering those provisions.

Liability. Volunteers would not be agents, employees, or contractors of the state and would have no authority to obligate the state to a third party. The state would not be liable to a volunteer for personal injury or property damage sustained by the volunteer as a result of participation in the team.

Volunteers who in good faith provided professional services in response to a cybersecurity event would not be liable for civil damages as a result of their acts or omissions in providing such services, except for willful and wanton misconduct. This immunity would be limited to services provided during the time of deployment for a cybersecurity event.

Confidential information. Information written, produced, collected, assembled, or maintained by DIR, a participating entity, the cybersecurity council, or a volunteer in the implementation of the bill's provisions related to the volunteer incident response team would be confidential and not subject to disclosure under public information laws if:

- the information contained certain identifying information;
- consisted of a participating entity's cybersecurity plans or cybersecurity-related practices; or
- was obtained from a participating entity or the entity's computer system in the course of providing assistance.

Report. No later than October 15, 2022, DIR would have to submit a report on the department's activities and recommendations related to the Texas Volunteer Incident Response Team to the House and Senate standing committees with primary jurisdiction over state agency cybersecurity.

Regional network security centers. CSSB 475 would authorize DIR to establish regional network security centers under the department's managed security services framework to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other eligible entities that elected to participate in and receive services through the center. DIR could establish more than one regional network security center only if it determined the first center successfully provided the services it had been contracted to provide to state agencies and other eligible entities.

DIR would have to enter into an interagency contract or interlocal contract, as appropriate, with an eligible participating entity that elected to participate in and receive services through a regional network security center.

Center locations, security. In creating and operating a regional network security center, DIR would have to partner with a university system or institution of higher education, other than a public junior college, to serve as an education partner with DIR for the center. The system or institution would have to enter into an interagency contract with DIR.

A university system or institution of higher education selected to serve as a regional network security center would be required to control and monitor all entrances to and critical areas of the center to prevent

unauthorized entry. Access would have to be restricted to only authorized individuals, and a local law enforcement agency or other security entity would have to monitor security alarms at the center, subject to service availability. DIR and a university system or institution of higher education selected to serve as a center would have to restrict operational information only to center personnel, except as provided by under the Government Code.

Center services and support. Under the bill, DIR could offer certain managed security services through a regional network security center, including:

- real-time network security monitoring to detect and respond to network security events that could jeopardize the state and its residents;
- alerts and guidance for defeating network security threats;
- immediate response to counter network security activity that exposed the state and its residents to risk;
- development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and mitigate the impact of network security incidents for participating entities; and
- cybersecurity educational services.

Guidelines and operating procedures. DIR would have to adopt and provide to each regional network security center appropriate network security guidelines and standard operating procedures to ensure efficient operation and maximum return on the state's investment. DIR would have to revise the procedures as necessary to confirm network security, and each eligible entity that participated in a center would have to comply with the network security guidelines and standard operating procedures.

Data management officers. CSSB 475 would require each state agency with more than 150 full-time employees to designate a full-time employee of the agency to serve as a data management officer.

The data management officer for a state agency would be required to:

- coordinate with the chief data officer of DIR to ensure the agency performed the duties assigned by statute;
- establish an agency data governance program to identify the agency's data assets and oversee those assets; and
- coordinate with the agency's information security officer, the agency's records management officer, and the Texas State Library and Archives Commission to implement best practices for managing and securing data in accordance with state privacy laws and data privacy classification, conduct a data maturity assessment of the agency's data governance program, and fulfill other duties as specified in the bill.

Each state agency would have to designate a data management officer as soon as practicable after the effective date of the bill.

Agency information security assessment, report. The bill would require each state agency's biennial information security assessment to include an assessment of the agency's data governance program with the participation of the data management officer, if applicable, and in accordance requirements established by DIR rule.

CSSB 475 also would change the reporting deadline for the results of the assessment from December 1 of the year in which the assessment was conducted to November 15 of each even-numbered year. DIR would be required, rather than permitted, to establish requirements for such assessments and the report, and the report and all related documentation would be confidential and not subject to disclosure under public information laws.

Data management advisory committee. The bill would require the board of DIR to appoint a data management advisory committee composed of its chief data officer and each state agency's data management officer. The committee would have to:

- advise the board and DIR on establishing statewide data ethics,

principles, goals, strategies, standards, and architecture;
- provide guidance and recommendations on governing and managing state agency data and data management systems; and
- establish performance objectives for state agencies from this state's data-driven policy goals.

Government Code provisions governing the composition and duration of advisory committees would not apply to the data management advisory committee.

Managed security services framework. The bill would require DIR to establish a framework for regional cybersecurity working groups to execute mutual aid agreements that allowed state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the Texas Volunteer Incident Response Team to assist with responding to a cybersecurity event in the state. Working groups could be established within the geographic area of a regional planning commission, and groups could establish a list of available cybersecurity experts and share resources to assist in responding to and recovering from the cybersecurity event.

DIR would have to establish the framework by December 1, 2021.

Restrictions on use of certain identifying information. The bill would prohibit a state agency from using global positioning system technology, individual contact tracing, or technology designed to obtain biometric identifiers to acquire information that alone or in conjunction with other information identified an individual or their location without the individual's consent. State agencies also could not retain such information about an individual or disseminate such information about an individual to another person unless the state agency first obtained the individual's written or electronic consent.

A state agency could acquire, retain, and disseminate such information about an individual without the individual's consent if the acquisition,

retention, or dissemination was required or permitted by a federal statute or certain state statute or was made by or to a law enforcement agency for a law enforcement purpose.

A state agency would have to retain the written or electronic consent of an individual in the agency's records until the contract or agreement under which the information was acquired, retained, or disseminated expired.

Other provisions. The bill would require each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency to include in the contract a provision requiring the vendor to meet the security controls the agency determined were proportionate with the agency's risk based on the sensitivity of the data. The vendor would have to periodically provide the agency with evidence that the vendor met the security controls.

On initiation of an information resources technology project, a state agency would have to classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements.

The bill also would include robotic process automation among the next generation technologies state agencies and local governments would have to consider using in their administration.

The bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2021. The bill would apply only to information acquired, retained, or disseminated by a state agency to another person on or after its effective date, and state agencies would have to ensure information resources technology projects initiated on or after that date complied with the bill's requirements.

NOTES:

According to the Legislative Budget Board, the bill would have no significant implication to the state. However, the bill would authorize the Texas Department of Information Resources to establish regional security

centers, and if the department did so, there would be an indeterminate cost to the state.