BILL ANALYSIS

C.S.S.B. 475
By: Nelson
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The legislature has made significant strides in improving the state's cybersecurity posture in recent years. During the most recent interim, the Texas Cybersecurity Council and the Texas Privacy Protection Advisory Council made recommendations to further improve cybersecurity standards and improve data management practices for state agencies and local governments. C.S.S.B. 475 seeks to implement certain recommendations from those entities by addressing third-party provider's security; establishing a volunteer cybersecurity incidence response team; establishing a regional network security center; implementing best practices for managing and securing data; and prohibiting state agencies from acquiring, retaining, or disseminating data used to identify an individual or the individual's location without written consent.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Department of Information Resources in SECTIONS 2, 4, 6, and 7 of this bill.

ANALYSIS

C.S.S.B. 475 amends the Government Code to set out provisions relating to state agency and local government information management and security.

Data Management Advisory Committee

C.S.S.B. 475 requires the governing board of the Department of Information Resources (DIR) to appoint a data management advisory committee to do the following:

- 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 applicable state agencies from the state's data-driven policy goals.

The bill sets out the composition of the advisory committee and exempts the advisory committee from provisions governing the composition and duration of state agency advisory committees generally.

Cloud Computing State Risk and Authorization Management Program

C.S.S.B. 475 requires DIR, not later than 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 process the data of an applicable state agency. The bill requires the program to allow a vendor to demonstrate compliance by submitting documentation that shows the vendor's compliance with a risk and authorization management program of the federal government or another state that DIR approves. The bill requires DIR by rule to prescribe the following:

- the categories and characteristics of cloud computing services subject to the program; and
- the requirements for certification through the program of vendors that provide those services.

C.S.S.B. 475 requires an applicable state agency to require each vendor contracting with the agency to provide cloud computing services for the agency to comply with the requirements of the program and requires DIR to evaluate vendors to determine whether a vendor qualifies for a certification issued by DIR reflecting compliance with program requirements. The bill prohibits an agency from entering into or renewing such a contract unless the vendor demonstrates compliance with program requirements and requires the agency to require the vendor to maintain program compliance and certification throughout the term of the contract. The bill requires an agency to ensure that each contract for cloud computing services the agency enters into or renews on or after January 1, 2022, complies with these applicable bill provisions.

Managed Security Services Framework

C.S.S.B. 475 requires DIR, not later than December 1, 2021, to establish a framework for regional cybersecurity working groups to execute mutual aid agreements that allow applicable 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 Texas. The bill provides that a working group may be established within the geographic area of a regional planning commission and authorizes a working group to establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity event and recovery from the event.

Designated Data Management Officers

C.S.S.B. 475 requires each executive or judicial branch state agency with more than 150 full-time employees to designate a full-time agency employee to serve as a data management officer and requires the officer to do the following:

- coordinate with the agency's chief data officer to ensure the agency performs the duties assigned to the chief data officer;
- in accordance with DIR guidelines, establish an agency data governance program to identify the agency's data assets, exercise authority and management over the agency's data assets, and establish related processes and procedures to oversee the agency's data 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 do the following:
    - implement best practices for managing and securing data in accordance with state privacy laws and data privacy classifications;
    - ensure the agency's records management programs apply to all types of data storage media;
    - increase awareness of and outreach for the agency's records management programs within the agency; and
    - conduct a data maturity assessment of the agency's data governance program in accordance with the requirements established by DIR rule.

The bill requires the officer, in accordance with DIR guidelines, to post on the Texas Open Data Portal at least three high-value data sets and prohibits the posted data sets from including information that is confidential or protected from disclosure under state or federal law. The bill authorizes the officer to delegate in writing to another agency employee the duty to implement a specific requirement assigned to the officer or to participate in the data management advisory committee.

Security Controls for State Agency Data

C.S.S.B. 475 requires each applicable state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency to include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. The bill requires the vendor to periodically provide to the agency evidence that the vendor meets the security controls required under the contract.

Data Classification, Security, and Retention Requirements

C.S.S.B. 475 requires an applicable state agency, on initiation of an information resources technology project, to classify the data produced from or used in the project and determine appropriate data security and an applicable records retention schedule for each classification.

Texas Volunteer Incident Response Team

C.S.S.B. 475 requires DIR, not later than December 1, 2021, to establish the Texas volunteer incident response team to provide rapid response assistance to an applicable state agency or local government under DIR direction during a cybersecurity event. The bill requires DIR to prescribe eligibility criteria for participation as a volunteer to provide that rapid response assistance, including a requirement that each volunteer have expertise in addressing cybersecurity events.

C.S.S.B. 475 requires DIR to enter into a contract with each volunteer approved to provide rapid response assistance and sets out requirements for the content of such a contract. The bill requires DIR to require criminal history record information for each individual who accepts an invitation to become a volunteer and authorizes DIR to request other information relevant to an individual's qualification and fitness to serve as a volunteer. The bill establishes that DIR has sole discretion to determine whether an individual is qualified to serve as a volunteer.

C.S.S.B. 475 authorizes DIR, on request of an agency or local government participating and receiving assistance from the response team, and in response to a cybersecurity event that affects multiple such participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, to deploy volunteers and provide rapid response assistance under DIR's direction and the managed security services framework established by the bill to assist with the event. The bill establishes that a volunteer may only accept a deployment in writing and that a volunteer may decline to accept a deployment for any reason.

C.S.S.B. 475 requires the cybersecurity council to review and make recommendations to DIR regarding the policies and procedures used by DIR to implement the bill's provisions establishing the response team and authorizes DIR to consult with the council to implement and administer those provisions.

C.S.S.B. 475 requires DIR to do the following with respect to the response team:

- approve the incident response tools the team may use in responding to a cybersecurity event;
- establish the eligibility criteria an individual must meet to become a volunteer;
- develop and publish guidelines for operation of the incident response team; and

- adopt rules necessary to implement the bill's provisions establishing the team.

The bill authorizes DIR to do the following with respect to the response team:

- require a participating entity to enter into a contract as a condition for obtaining assistance from the team that complies with the requirements of the Interagency Cooperation Act and other applicable state law;
- provide appropriate training to prospective and approved volunteers;
- in accordance with state law, provide compensation for certain expenses incurred by a volunteer on a deployment using money available for that purpose; and
- establish a fee schedule for participating entities receiving incident response team assistance.

C.S.S.B. 475 establishes that a volunteer is not an agent, employee, or independent contractor of the state for any purpose and has no authority to obligate the state to a third party. The bill provides that the state is not liable to a volunteer for personal injury or property damage sustained by the volunteer that arises from participation in the team. The bill grants a volunteer who in good faith provides professional services in response to a cybersecurity event immunity from civil liability as a result of the volunteer's acts or omissions in providing the services, except with respect to wilful and wanton misconduct, and limits this immunity to services provided during the time of deployment for a cybersecurity event.

C.S.S.B. 475 makes confidential and excepted from disclosure under state public information law information written, produced, collected, assembled, or maintained by DIR, a participating entity, the cybersecurity council, or a volunteer relating to the response team if the information:

- contains the contact information of a volunteer;
- identifies or provides a means of identifying a person who may, as a result of disclosure of the information, become a victim of a cybersecurity event;
- consists of a participating entity's cybersecurity plans or cybersecurity-related practices; or
- is obtained from a participating entity or from a participating entity's computer system in the course of providing assistance through the team.

C.S.S.B. 475 requires DIR, not later than October 15, 2022, to submit to the applicable legislative standing committees a report on DIR's activities and recommendations related to the response team.

Agency Information Security Assessment and Report

C.S.S.B. 475 requires the applicable state agency's biennial information security assessment to include an assessment of the agency's data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by DIR rule. With respect to that assessment and the corresponding report of the assessment's results, the bill does the following:

- replaces the authorization for DIR to establish the requirements for the assessment and report by rule with a requirement for DIR to do so;
- changes the deadline by which the agency must submit the report from December 1 of each year in which the agency conducts the assessment to November 15 of each even-numbered year;
- makes the report and all documentation related to the assessment and report confidential and not subject to disclosure under state public information law; and
- authorizes the agency or DIR to redact or withhold the information as such without requesting a decision from the attorney general.

Use of Next Generation Technology

C.S.S.B. 475 includes robotic process automation among the next generation technologies each applicable state agency and local government must consider using in the administration of the agency or government.

Regional Network Security Centers

C.S.S.B. 475 authorizes DIR to establish regional network security centers, under the DIR managed security services framework, to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other governmental entities eligible to receive network security services from DIR, other than a school district or hospital district, that elect to participate in and receive services through the center. DIR may establish more than one center only if DIR determines the first center established successfully provides to state agencies and those other eligible entities the services the center has contracted to provide. The bill requires DIR to enter into an interagency contract or an interlocal contract, as appropriate, with an eligible participating entity that elects to participate in and receive services through a regional network security center.

C.S.S.B. 475 requires DIR, in creating and operating a regional network security center, to partner with a university system or public institution of higher education, other than a public junior college. The bill requires the system or institution to serve as an education partner with DIR for the center and to enter into an interagency contract with DIR. The bill requires DIR, in selecting a center's location, to select a system or institution that has supportive educational capabilities. The bill requires a system or institution selected to serve as a center to control and monitor all entrances to and critical areas of the center to prevent unauthorized entry. The bill requires the system or institution to restrict access to the center to only authorized individuals. The bill requires a local law enforcement entity or any entity providing security for such a center to monitor security alarms at the center subject to the availability of that service. The bill requires DIR and an entity selected to serve as a center to restrict operational information to only center personnel, except as provided by provisions relating to a state audit.

C.S.S.B. 475 authorizes DIR to offer the following managed security services through a regional network security center:

- real-time network security monitoring to detect and respond to network security events that may jeopardize the state and Texas residents;
- alerts and guidance for defeating network security threats;
- immediate response to counter network security activity that exposes Texas 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.

C.S.S.B. 475 requires DIR to adopt and provide to each regional network security center appropriate network security guidelines and standard operating procedures to ensure efficient operation of the center with a maximum return on the state's investment. The bill requires DIR to revise those procedures as necessary to confirm network security and requires each eligible participating entity that elects to participate in a center to comply with the applicable guidelines and procedures.

Restrictions on State Agency Use of Certain Individual-Identifying Information

C.S.S.B. 475, effective September 1, 2021, prohibits a state agency from doing any of the following:

- 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 identifies an individual or the individual's location without the individual's written or electronic consent;

- retaining information with respect to such an individual without the individual's written or electronic consent; or
- disseminating to a person such information with respect to an individual unless the agency first obtains the individual's written or electronic consent.

The bill requires an agency to retain the written or electronic consent of an individual in the agency's records until the contract or agreement under which the information is acquired, retained, or disseminated expires.

C.S.S.B. 475 authorizes a state agency to acquire, retain, and disseminate such individual-identifying information with respect to an individual without the individual's written or electronic consent if the acquisition, retention, or dissemination is required or permitted by a federal law or by a state law other than state public information law or is made by or to a law enforcement agency for a law enforcement purpose.

EFFECTIVE DATE

Except as otherwise provided, on passage, or, if the bill does not receive the necessary vote, September 1, 2021.

COMPARISON OF SENATE ENGROSSED AND SUBSTITUTE

While C.S.S.B. 475 may differ from the engrossed in minor or nonsubstantive ways, the following summarizes the substantial differences between the engrossed and committee substitute versions of the bill.

The substitute includes an authorization not in the engrossed for a state agency's data management officer to delegate in writing certain of the officer's duties to another agency employee.