BILL ANALYSIS

Senate Research Center
87R18280 YDB-D

C.S.S.B. 475
By: Nelson
Finance
4/7/2021
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The legislature has made significant strides in improving the state's cybersecurity posture. During the interim the Texas Cybersecurity Council and the Texas Privacy Protection Advisory Council made recommendations to further improve cybersecurity standards and improve data management.

S.B. 475 implements recommendations from both by addressing third party provider's security, establishing a volunteer cybersecurity incidence response team, 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.

(Original Author's/Sponsor's Statement of Intent)

C.S.S.B. 475 amends current law relating to state agency and local government information management and security, including establishment of the state risk and authorization management program and the Texas volunteer incident response team, and authorizes fees.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Texas Department of Information Resources in SECTION 2 (Section 2054.0593, Government Code) and SECTION 6 (Section 2054.52007, Government Code) of this bill.

Rulemaking authority previously granted to Texas Department of Information Resources is modified in SECTION 7 (Section 2054.515, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter B, Chapter 2054, Government Code, by adding Section 2054.0332, as follows:

> Sec. 2054.0332. DATA MANAGEMENT ADVISORY COMMITTEE. (a) Requires the governing board of the Department of Information Resources (board) to appoint a data management advisory committee.
>
> (b) Provides that the advisory committee is composed of each data management officer designated by a state agency under Section 2054.137 and the chief data officer of the Department of Information Resources (DIR).
>
> (c) Requires the advisory committee to:
>
> (1) advise the board and DIR on establishing statewide data ethics, principles, goals, strategies, standards and architecture;
>
> (2) provide guidance and recommendations on governing and managing state agency data and data management systems, including

recommendations to assist data management officers in fulfilling the duties assigned under Section 2054.137; and

(3) establish performance objectives for state agencies from this state's data-driven policy goals.

(d) Provides that Sections 2110.002 (Composition of Advisory Committee) and 2110.008 (Duration of Advisory Committee) do not apply to the advisory committee.

SECTION 2. Amends Subchapter C, Chapter 2054, Government Code, by adding Section 2054.0593, as follows:

Sec. 2054.0593. CLOUD COMPUTING STATE RISK AND AUTHORIZATION MANAGEMENT PROGRAM. (a) Defines "cloud computing service."

(b) Requires DIR 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 a state agency. Requires that the program allow a vendor to demonstrate compliance by submitting documentation that shows the vendor's compliance with a risk and authorization management program of:

(1) the federal government; or

(2) another state that DIR approves.

(c) Requires DIR to prescribe by rule the categories and characteristics of cloud computing services subject to the state risk and authorization management program, and to prescribe the requirements for certification through the program of vendors that provide cloud computing services.

(d) Requires a 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 state risk and authorization management program. Requires DIR to evaluate vendors to determine whether a vendor qualifies for a certification issued by DIR reflecting compliance with program requirements.

(e) Prohibits a state agency from entering or renewing a contract with a vendor to purchase cloud computing services for the agency that are subject to the state risk and authorization management program unless the vendor demonstrates compliance with program requirements.

(f) Requires a state agency to require a vendor contracting with the agency to provide cloud computing services for the agency that are subject to the state risk and authorization management program to maintain program compliance and certification throughout the term of the contract.

SECTION 3. Amends Section 2054.0594, Government Code, by adding Subsection (d), as follows:

(d) Requires DIR to establish a framework for regional cybersecurity working groups to execute mutual aid agreements that allow state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the incident response team established under Subchapter N-2 to assist with responding to a cybersecurity event in this state. Authorizes a working group to be established within the geographic area of a regional planning commission established under Chapter 391 (Regional Planning Commissions), Local Government Code. Authorizes the 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.

SECTION 4. Amends Subchapter F, Chapter 2054, Government Code, by adding Sections 2054.137 and 2054.138, as follows:

Sec. 2054.137. DESIGNATED DATA MANAGEMENT OFFICER. (a) Requires 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.

(b) Requires the data management officer for a state agency to:

(1) coordinate with the chief data officer to ensure the agency performs the duties assigned under Section 2054.0286 (Chief Data Officer);

(2) 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

(3) coordinate with the agency's information security officer, the agency's records management officer, and the Texas State Library and Archives Commission to:

(A) implement best practices for managing and securing data in accordance with state privacy laws and data privacy classifications;

(B) ensure the agency's records management programs apply to all types of data storage media; and

(C) increase awareness of and outreach for the agency's records management programs within the agency; and

(D) conduct a data maturity assessment of the agency's data governance program in accordance with the requirements established by DIR rule.

(c) Requires the data management officer for the state agency, in accordance with DIR guidelines, to post on the Texas Open Data Portal established by DIR under Section 2054.070 (Central Repository for Publicly Accessible Electronic Data) at least three high-value data sets as defined by Section 2054.1265 (Posting High-Value Data Sets on Internet). Prohibits the high-value data sets from including information that is confidential or protected from disclosure under state or federal law.

Sec. 2054.138. SECURITY CONTROLS FOR STATE AGENCY DATA. Requires that each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use or store data for the agency 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. Requires the vendor to periodically provide to the agency evidence that the vendor meets the security controls required under the contract.

SECTION 5. Amends Subchapter G, Chapter 2054, Government Code, by adding Section 2054.161, as follows:

Sec. 2054.161. DATA CLASSIFICATION, SECURITY, AND RETENTION REQUIREMENTS. Requires a state agency, on initiation of an information resources technology project, including an application development project and any information resources projects described in Subchapter G (Project Management Practices), to classify

the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Section 441.185 (Record Retention Schedules) for each classification.

SECTION 6. Amends Chapter 2054, Government Code, by adding Subchapter N-2, as follows:

SUBCHAPTER N-2. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2054.52001. DEFINITIONS. Defines "incident response team," "participating entity," and "volunteer."

Sec. 2054.52002. ESTABLISHMENT OF TEXAS VOLUNTEER INCIDENT RESPONSE TEAM. (a) Requires DIR to establish the Texas volunteer incident response team to provide rapid response assistance to a participating entity under DIR's direction during a cybersecurity event.

(b) Requires DIR 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.

Sec. 2054.52003. CONTRACT WITH VOLUNTEERS. Requires DIR to enter into a contract with each volunteer DIR approves to provide rapid response assistance under this subchapter. Requires that the contract require the volunteer to agree to certain terms and procedures.

Sec. 2054.52004. VOLUNTEER QUALIFICATION. (a) Requires DIR to require criminal history record information for each individual who accepts an invitation to become a volunteer.

(b) Authorizes DIR to request other information relevant to the individual's qualification and fitness to serve as a volunteer.

(c) Provides that DIR has sole discretion to determine whether an individual is qualified to serve as a volunteer.

Sec. 2054.52005. DEPLOYMENT. (a) Authorizes DIR, in response to a cybersecurity event that affects multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, on request of a participating entity, to deploy volunteers and provide rapid response assistance under DIR's direction and the managed security services framework established under Section 2054.0594(d) to assist with the event.

(b) Authorizes a volunteer to only accept a deployment under this subchapter in writing. Authorizes a volunteer to decline to accept a deployment for any reason.

Sec. 2054.52006. CYBERSECURITY COUNCIL DUTIES. Requires the cybersecurity council established under Section 2054.512 (Cybersecurity Council) to review and make recommendations to DIR regarding the policies and procedures used by DIR to implement this subchapter. Authorizes DIR to consult with the council to implement and administer this subchapter.

Sec. 2054.52007. DEPARTMENT POWERS AND DUTIES. (a) Requires DIR to:

(1) approve the incident response tools the incident response team is authorized to use in responding to a cybersecurity event;

(2) establish the eligibility criteria an individual is required to meet to become a volunteer;

(3) develop and publish guidelines for operation of the incident response team, including the:

(A) standards and procedures DIR uses to determine whether an individual is eligible to serve as a volunteer;

(B) process for an individual to apply for and accept incident response team membership;

(C) requirements for a participating entity to receive assistance from the incident response team; and

(D) process for a participating entity to request and obtain the assistance of the incident response team; and

(4) adopt rules necessary to implement this subchapter.

(b) Authorizes DIR to require a participating entity to enter into a contract as a condition for obtaining assistance from the incident response team. Requires that the contract comply with the requirements of Chapters 771 (Interagency Cooperation Act) and 791 (Interlocal Cooperation Contracts).

(c) Authorizes DIR to provide appropriate training to prospective and approved volunteers.

(d) Authorizes DIR, in accordance with state law, to provide compensation for actual and necessary travel and living expenses incurred by a volunteer on a deployment using money available for that purpose.

(e) Authorizes DIR to establish a fee schedule for participating entities receiving incident response team assistance. Prohibits the amount of fees collected from exceeding DIR's costs to operate the incident response team.

Sec. 2054.52008. STATUS OF VOLUNTEER; LIABILITY. (a) Provides that a volunteer is not an agent, employee, or independent contractor of this state for any purpose and has no authority to obligate this state to a third party.

(b) Provides that this state is not liable to a volunteer for personal injury or property damage sustained by the volunteer that arises from participation in the incident response team.

Sec. 2054.52009. CIVIL LIABILITY. Provides that a volunteer who in good faith provides professional services in response to a cybersecurity event is not liable for civil damages as a result of the volunteer's acts or omissions in providing the services, except for wilful and wanton misconduct. Provides that this immunity is limited to services provided during the time of deployment for a cybersecurity event.

Sec. 2054.52010. CONFIDENTIAL INFORMATION. Provides that information written, produced, collected, assembled, or maintained by DIR, a participating entity, the cybersecurity council, or a volunteer in the implementation of this subchapter is confidential and not subject to disclosure under Chapter 552 (Public Information) if the information contains certain types of protected information.

SECTION 7. Amends Section 2054.515, Government Code, as follows:

Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) Requires each state agency, at least once every two years, to conduct an information security assessment of the agency's:

(1) creates this subdivision from existing text and makes a nonsubstantive change; and

(2) data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by DIR rule.

(b) Requires a state agency, not later than November 15 of each even-numbered year, rather than December 1 of the year in which a state agency conducts the assessment under Subsection (a), to report the results of the assessment to certain entities.

(c) Requires, rather than authorizes, DIR by rule to establish the requirements for the information security assessment and report required by this section.

(d) Provides that the report and all documentation related to the information security assessment and report are confidential and not subject to disclosure under Chapter 552. Authorizes the state agency or department to redact or withhold the information as confidential under Chapter 552 without requesting a decision from the attorney general under Subchapter G (Attorney General Decisions), Chapter 552.

SECTION 8. Amends Section 2054.601, Government Code, as follows:

Sec. 2054.601. USE OF NEXT GENERATION TECHNOLOGY. Requires that each state agency and local government, in the administration of the agency or local government, consider using next generation technologies, including cryptocurrency, blockchain technology, robotic process automation, and artificial intelligence.

SECTION 9. Amends Chapter 2059, Government Code, by adding Subchapter E, as follows:

SUBCHAPTER E. REGIONAL NETWORK SECURITY CENTERS

Sec. 2059.201. ELIGIBLE PARTICIPATING ENTITIES. Provides that a state agency or an entity listed in Sections 2059.058(b)(3)-(5) (relating to DIR's authorization to provide network security to certain political subdivisions of this state, certain independent organizations, and public junior colleges) is eligible to participate in cybersecurity support and network security provided by a regional network security center under Subchapter E.

Sec. 2059.202. ESTABLISHMENT OF REGIONAL NETWORK SECURITY CENTERS. (a) Authorizes DIR, subject to Subsection (b), to establish regional network security centers, under DIR's managed security services framework established by Section 2054.0594(d), to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other eligible entities that elect to participate in and receive services through the center.

(b) Provides that DIR may establish more than one regional network security center only if DIR determines the first center established by DIR successfully provides to state agencies and other eligible entities the services the center has contracted to provide.

(c) Requires DIR to enter into an interagency contract in accordance with Chapter 771 or an interlocal contract in accordance with Chapter 791, as appropriate, with an eligible participating entity that elects to participate in and receive services through a regional network security center.

Sec. 2059.203. REGIONAL NETWORK SECURITY CENTER LOCATIONS AND PHYSICAL SECURITY. (a) Requires DIR, in creating and operating a regional network security center, to partner with a university system or institution of higher education as

defined by Section 61.003 (Definitions), Education Code, other than a public junior college. Requires that the system or institution serve as an education partner with DIR for the regional network security center, and enter into an interagency contract with DIR in accordance with Chapter 771.

(b) Requires DIR, in selecting the location for a regional network security center, to select a university system or institution of higher education that has supportive educational capabilities.

(c) Requires a university system or institution of higher education selected to serve as a regional network security center to control and monitor all entrances to and critical areas of the center to prevent unauthorized entry. Requires that the system or institution restrict access to the center to only authorized individuals.

(d) Requires a local law enforcement entity or any entity providing security for a regional network security center to monitor security alarms at the regional network security center subject to the availability of that service.

(e) Requires DIR and a university system or institution of higher education selected to serve as a regional network security center to restrict operational information to only center personnel, except as provided by Chapter 321 (State Auditor).

Sec. 2059.204. REGIONAL NETWORK SECURITY CENTERS SERVICES AND SUPPORT. Authorizes DIR to offer the following managed security services through a regional network security center:

(1) real-time network security monitoring to detect and respond to network security events that may jeopardize this state and the residents of this state;

(2) alerts and guidance for defeating network security threats, including firewall configuration, installation, management, and monitoring, intelligence gathering, and protocol analysis;

(3) immediate response to counter network security activity that exposes this state and the residents of this state to risk, including complete intrusion detection system installation, management, and monitoring for participating entities;

(4) development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and mitigate the impact of network security incidents for participating entities; and

(5) cybersecurity educational services.

Sec. 2059.205. NETWORK SECURITY GUIDELINES AND STANDARD OPERATING PROCEDURES. (a) 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.

(b) Requires DIR to revise the standard operating procedures as necessary to confirm network security.

(c) Requires each eligible participating entity that elects to participate in a regional network security center to comply with the network security guidelines and standard operating procedures.

SECTION 10. Amends Subtitle B, Title 10, Government Code, by adding Chapter 2062, as follows:

CHAPTER 2062. RESTRICTIONS ON STATE AGENCY USE OF CERTAIN INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2062.001. DEFINITIONS. Defines "biometric identifier" and "state agency."

Sec. 2062.002. CONSENT REQUIRED BEFORE ACQUIRING, RETAINING, OR DISSEMINATING CERTAIN INFORMATION; RECORDS. (a) Prohibits a state agency, except as provided by Subsection (b), from:

(1) 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;

(2) retaining information with respect to an individual described by Subdivision (1) without the individual's written or electronic consent; or

(3) disseminating to a person the information described by Subdivision (1) with respect to an individual unless the state agency first obtains the individual's written or electronic consent.

(b) Authorizes a state agency to acquire, retain, and disseminate information described by Subsection (a) with respect to an individual without the individual's written or electronic consent if the acquisition, retention, or dissemination is:

(1) required or permitted by a federal statute or by a state statute other than Chapter 552; or

(2) made by or to a law enforcement agency for a law enforcement purpose.

(c) Requires a state agency to retain the written or electronic consent of an individual obtained as required under this section in the agency's records until the contract or agreement under which the information is acquired, retained, or disseminated expires.

SECTION 11. (a) Requires DIR, not later than December 1, 2021, to:

(1) establish the state risk and authorization management program as required by Section 2054.0593, Government Code, as added by this Act;

(2) establish the framework for regional cybersecurity working groups to execute mutual aid agreements as required under Section 2054.0594(d), Government Code, as added by this Act; and

(3) establish the Texas volunteer incident response team as required by Subchapter N-2, Chapter 2054, Government Code, as added by this Act.

(b) Requires each state agency to ensure that:

(1) each contract for cloud computing services the agency enters into or renews on or after January 1, 2022, complies with Section 2054.0593, Government Code, as added by this Act; and

(2) each contract subject to Section 2054.138, Government Code, as added by this Act, that is executed on or after the effective date of this Act complies with that section.

(c) Requires each state agency subject to Section 2054.137, Government Code, as added by this Act, to designate a data management officer as soon as practicable after the effective date of this Act.

(d) Requires each state agency subject to Section 2054.161, Government Code, as added by this Act, to ensure each information resources technology project initiated on or after the effective date of this Act complies with that section.

SECTION 12. Requires DIR, not later than October 15, 2022, to submit to the standing committees of the Texas Senate and Texas House of Representatives with primary jurisdiction over state agency cybersecurity a report on DIR's activities and recommendations related to the Texas volunteer incident response team established as required by Subchapter N-2, Chapter 2054, Government Code, as added by this Act.

SECTION 13. Makes application of Chapter 2062, as added by this Act, prospective.

SECTION 14. (a) Effective date, except as provided by Subsection (b) of this section: upon passage or September 1, 2021.

(b) Effective date, Chapter 2062, Government Code, as added by this Act: September 1, 2021.