

By: Nelson, et al.
(Capriglione)

S.B. No. 475

Substitute the following for S.B. No. 475:

By: Paddie

C.S.S.B. No. 475

A BILL TO BE ENTITLED

AN ACT

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; authorizing fees.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subchapter B, Chapter 2054, Government Code, is amended by adding Section 2054.0332 to read as follows:

Sec. 2054.0332. DATA MANAGEMENT ADVISORY COMMITTEE. (a) The board shall appoint a data management advisory committee.

(b) The advisory committee is composed of each data management officer designated by a state agency under Section 2054.137 and the department's chief data officer.

(c) The advisory committee shall:

(1) advise the board and department 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) Sections 2110.002 and 2110.008 do not apply to the

1 advisory committee.

2 SECTION 2. Subchapter C, Chapter 2054, Government Code, is
3 amended by adding Section 2054.0593 to read as follows:

4 Sec. 2054.0593. CLOUD COMPUTING STATE RISK AND
5 AUTHORIZATION MANAGEMENT PROGRAM. (a) In this section, "cloud
6 computing service" has the meaning assigned by Section 2157.007.

7 (b) The department shall establish a state risk and
8 authorization management program to provide a standardized
9 approach for security assessment, authorization, and continuous
10 monitoring of cloud computing services that process the data of a
11 state agency. The program must allow a vendor to demonstrate
12 compliance by submitting documentation that shows the vendor's
13 compliance with a risk and authorization management program of:

14 (1) the federal government; or

15 (2) another state that the department approves.

16 (c) The department by rule shall prescribe:

17 (1) the categories and characteristics of cloud
18 computing services subject to the state risk and authorization
19 management program; and

20 (2) the requirements for certification through the
21 program of vendors that provide cloud computing services.

22 (d) A state agency shall require each vendor contracting
23 with the agency to provide cloud computing services for the agency
24 to comply with the requirements of the state risk and authorization
25 management program. The department shall evaluate vendors to
26 determine whether a vendor qualifies for a certification issued by
27 the department reflecting compliance with program requirements.

1 (e) A state agency may not enter or renew a contract with a
2 vendor to purchase cloud computing services for the agency that are
3 subject to the state risk and authorization management program
4 unless the vendor demonstrates compliance with program
5 requirements.

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

11 SECTION 3. Section 2054.0594, Government Code, is amended
12 by adding Subsection (d) to read as follows:

13 (d) The department shall establish a framework for regional
14 cybersecurity working groups to execute mutual aid agreements that
15 allow state agencies, local governments, regional planning
16 commissions, public and private institutions of higher education,
17 the private sector, and the incident response team established
18 under Subchapter N-2 to assist with responding to a cybersecurity
19 event in this state. A working group may be established within the
20 geographic area of a regional planning commission established under
21 Chapter 391, Local Government Code. The working group may establish
22 a list of available cybersecurity experts and share resources to
23 assist in responding to the cybersecurity event and recovery from
24 the event.

25 SECTION 4. Subchapter F, Chapter 2054, Government Code, is
26 amended by adding Sections 2054.137 and 2054.138 to read as
27 follows:

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

2 Each state agency with more than 150 full-time employees shall
3 designate a full-time employee of the agency to serve as a data
4 management officer.

5 (b) The data management officer for a state agency shall:

6 (1) coordinate with the chief data officer to ensure
7 the agency performs the duties assigned under Section [2054.0286](#);

8 (2) in accordance with department guidelines,
9 establish an agency data governance program to identify the
10 agency's data assets, exercise authority and management over the
11 agency's data assets, and establish related processes and
12 procedures to oversee the agency's data assets; and

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

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

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

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

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

26 (c) In accordance with department guidelines, the data
27 management officer for a state agency shall post on the Texas Open

1 Data Portal established by the department under Section 2054.070 at
2 least three high-value data sets as defined by Section 2054.1265.
3 The high-value data sets may not include information that is
4 confidential or protected from disclosure under state or federal
5 law.

6 (d) The data management officer for a state agency may
7 delegate in writing to another agency employee the duty to:

8 (1) implement a specific requirement of Subsection (b)
9 or (c); or

10 (2) participate in the advisory committee established
11 under Section 2054.0332.

12 Sec. 2054.138. SECURITY CONTROLS FOR STATE AGENCY DATA.
13 Each state agency entering into or renewing a contract with a vendor
14 authorized to access, transmit, use, or store data for the agency
15 shall include a provision in the contract requiring the vendor to
16 meet the security controls the agency determines are proportionate
17 with the agency's risk under the contract based on the sensitivity
18 of the agency's data. The vendor must periodically provide to the
19 agency evidence that the vendor meets the security controls
20 required under the contract.

21 SECTION 5. Subchapter G, Chapter 2054, Government Code, is
22 amended by adding Section 2054.161 to read as follows:

23 Sec. 2054.161. DATA CLASSIFICATION, SECURITY, AND
24 RETENTION REQUIREMENTS. On initiation of an information resources
25 technology project, including an application development project
26 and any information resources projects described in this
27 subchapter, a state agency shall classify the data produced from or

1 used in the project and determine appropriate data security and
2 applicable retention requirements under Section 441.185 for each
3 classification.

4 SECTION 6. Chapter 2054, Government Code, is amended by
5 adding Subchapter N-2 to read as follows:

6 SUBCHAPTER N-2. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

7 Sec. 2054.52001. DEFINITIONS. In this subchapter:

8 (1) "Incident response team" means the Texas volunteer
9 incident response team established under Section 2054.52002.

10 (2) "Participating entity" means a state agency,
11 including an institution of higher education, or a local government
12 that receives assistance under this subchapter during a
13 cybersecurity event.

14 (3) "Volunteer" means an individual who provides rapid
15 response assistance during a cybersecurity event under this
16 subchapter.

17 Sec. 2054.52002. ESTABLISHMENT OF TEXAS VOLUNTEER INCIDENT
18 RESPONSE TEAM. (a) The department shall establish the Texas
19 volunteer incident response team to provide rapid response
20 assistance to a participating entity under the department's
21 direction during a cybersecurity event.

22 (b) The department shall prescribe eligibility criteria for
23 participation as a volunteer member of the incident response team,
24 including a requirement that each volunteer have expertise in
25 addressing cybersecurity events.

26 Sec. 2054.52003. CONTRACT WITH VOLUNTEERS. The department
27 shall enter into a contract with each volunteer the department

1 approves to provide rapid response assistance under this
2 subchapter. The contract must require the volunteer to:

3 (1) acknowledge the confidentiality of information
4 required by Section 2054.52010;

5 (2) protect all confidential information from
6 disclosure;

7 (3) avoid conflicts of interest that might arise in a
8 deployment under this subchapter;

9 (4) comply with department security policies and
10 procedures regarding information resources technologies;

11 (5) consent to background screening required by the
12 department; and

13 (6) attest to the volunteer's satisfaction of any
14 eligibility criteria established by the department.

15 Sec. 2054.52004. VOLUNTEER QUALIFICATION. (a) The
16 department shall require criminal history record information for
17 each individual who accepts an invitation to become a volunteer.

18 (b) The department may request other information relevant
19 to the individual's qualification and fitness to serve as a
20 volunteer.

21 (c) The department has sole discretion to determine whether
22 an individual is qualified to serve as a volunteer.

23 Sec. 2054.52005. DEPLOYMENT. (a) In response to a
24 cybersecurity event that affects multiple participating entities
25 or a declaration by the governor of a state of disaster caused by a
26 cybersecurity event, the department on request of a participating
27 entity may deploy volunteers and provide rapid response assistance

1 under the department's direction and the managed security services
2 framework established under Section 2054.0594(d) to assist with the
3 event.

4 (b) A volunteer may only accept a deployment under this
5 subchapter in writing. A volunteer may decline to accept a
6 deployment for any reason.

7 Sec. 2054.52006. CYBERSECURITY COUNCIL DUTIES. The
8 cybersecurity council established under Section 2054.512 shall
9 review and make recommendations to the department regarding the
10 policies and procedures used by the department to implement this
11 subchapter. The department may consult with the council to
12 implement and administer this subchapter.

13 Sec. 2054.52007. DEPARTMENT POWERS AND DUTIES. (a) The
14 department shall:

15 (1) approve the incident response tools the incident
16 response team may use in responding to a cybersecurity event;

17 (2) establish the eligibility criteria an individual
18 must meet to become a volunteer;

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

21 (A) standards and procedures the department uses
22 to determine whether an individual is eligible to serve as a
23 volunteer;

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

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

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

3 (4) adopt rules necessary to implement this
4 subchapter.

5 (b) The department may require a participating entity to
6 enter into a contract as a condition for obtaining assistance from
7 the incident response team. The contract must comply with the
8 requirements of Chapters 771 and 791.

9 (c) The department may provide appropriate training to
10 prospective and approved volunteers.

11 (d) In accordance with state law, the department may provide
12 compensation for actual and necessary travel and living expenses
13 incurred by a volunteer on a deployment using money available for
14 that purpose.

15 (e) The department may establish a fee schedule for
16 participating entities receiving incident response team
17 assistance. The amount of fees collected may not exceed the
18 department's costs to operate the incident response team.

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

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

26 Sec. 2054.52009. CIVIL LIABILITY. A volunteer who in good
27 faith provides professional services in response to a cybersecurity

1 event is not liable for civil damages as a result of the volunteer's
2 acts or omissions in providing the services, except for wilful and
3 wanton misconduct. This immunity is limited to services provided
4 during the time of deployment for a cybersecurity event.

5 Sec. 2054.52010. CONFIDENTIAL INFORMATION. Information
6 written, produced, collected, assembled, or maintained by the
7 department, a participating entity, the cybersecurity council, or a
8 volunteer in the implementation of this subchapter is confidential
9 and not subject to disclosure under Chapter 552 if the information:

10 (1) contains the contact information for a volunteer;

11 (2) identifies or provides a means of identifying a
12 person who may, as a result of disclosure of the information, become
13 a victim of a cybersecurity event;

14 (3) consists of a participating entity's cybersecurity
15 plans or cybersecurity-related practices; or

16 (4) is obtained from a participating entity or from a
17 participating entity's computer system in the course of providing
18 assistance under this subchapter.

19 SECTION 7. Section 2054.515, Government Code, is amended to
20 read as follows:

21 Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND
22 REPORT. (a) At least once every two years, each state agency shall
23 conduct an information security assessment of the agency's:

24 (1) information resources systems, network systems,
25 digital data storage systems, digital data security measures, and
26 information resources vulnerabilities; and

27 (2) data governance program with participation from

1 the agency's data management officer, if applicable, and in
2 accordance with requirements established by department rule.

3 (b) Not later than November 15 of each even-numbered year
4 ~~[December 1 of the year in which a state agency conducts the~~
5 ~~assessment under Subsection (a)]~~, the agency shall report the
6 results of the assessment to:

7 (1) the department; and

8 (2) on request, the governor, the lieutenant governor,
9 and the speaker of the house of representatives.

10 (c) The department by rule shall ~~may~~ establish the
11 requirements for the information security assessment and report
12 required by this section.

13 (d) The report and all documentation related to the
14 information security assessment and report are confidential and not
15 subject to disclosure under Chapter 552. The state agency or
16 department may redact or withhold the information as confidential
17 under Chapter 552 without requesting a decision from the attorney
18 general under Subchapter G, Chapter 552.

19 SECTION 8. Section 2054.601, Government Code, is amended to
20 read as follows:

21 Sec. 2054.601. USE OF NEXT GENERATION TECHNOLOGY. Each
22 state agency and local government shall, in the administration of
23 the agency or local government, consider using next generation
24 technologies, including cryptocurrency, blockchain technology,
25 robotic process automation, and artificial intelligence.

26 SECTION 9. Chapter 2059, Government Code, is amended by
27 adding Subchapter E to read as follows:

1 SUBCHAPTER E. REGIONAL NETWORK SECURITY CENTERS

2 Sec. 2059.201. ELIGIBLE PARTICIPATING ENTITIES. A state
3 agency or an entity listed in Sections 2059.058(b)(3)-(5) is
4 eligible to participate in cybersecurity support and network
5 security provided by a regional network security center under this
6 subchapter.

7 Sec. 2059.202. ESTABLISHMENT OF REGIONAL NETWORK SECURITY
8 CENTERS. (a) Subject to Subsection (b), the department may
9 establish regional network security centers, under the
10 department's managed security services framework established by
11 Section 2054.0594(d), to assist in providing cybersecurity support
12 and network security to regional offices or locations for state
13 agencies and other eligible entities that elect to participate in
14 and receive services through the center.

15 (b) The department may establish more than one regional
16 network security center only if the department determines the first
17 center established by the department successfully provides to state
18 agencies and other eligible entities the services the center has
19 contracted to provide.

20 (c) The department shall enter into an interagency contract
21 in accordance with Chapter 771 or an interlocal contract in
22 accordance with Chapter 791, as appropriate, with an eligible
23 participating entity that elects to participate in and receive
24 services through a regional network security center.

25 Sec. 2059.203. REGIONAL NETWORK SECURITY CENTER LOCATIONS
26 AND PHYSICAL SECURITY. (a) In creating and operating a regional
27 network security center, the department shall partner with a

1 university system or institution of higher education as defined by
2 Section 61.003, Education Code, other than a public junior college.

3 The system or institution shall:

4 (1) serve as an education partner with the department
5 for the regional network security center; and

6 (2) enter into an interagency contract with the
7 department in accordance with Chapter 771.

8 (b) In selecting the location for a regional network
9 security center, the department shall select a university system or
10 institution of higher education that has supportive educational
11 capabilities.

12 (c) A university system or institution of higher education
13 selected to serve as a regional network security center shall
14 control and monitor all entrances to and critical areas of the
15 center to prevent unauthorized entry. The system or institution
16 shall restrict access to the center to only authorized individuals.

17 (d) A local law enforcement entity or any entity providing
18 security for a regional network security center shall monitor
19 security alarms at the regional network security center subject to
20 the availability of that service.

21 (e) The department and a university system or institution of
22 higher education selected to serve as a regional network security
23 center shall restrict operational information to only center
24 personnel, except as provided by Chapter 321.

25 Sec. 2059.204. REGIONAL NETWORK SECURITY CENTERS SERVICES
26 AND SUPPORT. The department may offer the following managed
27 security services through a regional network security center:

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

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

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

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

16 (5) cybersecurity educational services.

17 Sec. 2059.205. NETWORK SECURITY GUIDELINES AND STANDARD
18 OPERATING PROCEDURES. (a) The department shall adopt and provide
19 to each regional network security center appropriate network
20 security guidelines and standard operating procedures to ensure
21 efficient operation of the center with a maximum return on the
22 state's investment.

23 (b) The department shall revise the standard operating
24 procedures as necessary to confirm network security.

25 (c) Each eligible participating entity that elects to
26 participate in a regional network security center shall comply with
27 the network security guidelines and standard operating procedures.

1 SECTION 10. Subtitle B, Title 10, Government Code, is
2 amended by adding Chapter 2062 to read as follows:

3 CHAPTER 2062. RESTRICTIONS ON STATE AGENCY USE OF CERTAIN

4 INDIVIDUAL-IDENTIFYING INFORMATION

5 Sec. 2062.001. DEFINITIONS. In this chapter:

6 (1) "Biometric identifier" has the meaning assigned by
7 Section 560.001.

8 (2) "State agency" means a department, commission,
9 board, office, council, authority, or other agency in the
10 executive, legislative, or judicial branch of state government,
11 including a university system or institution of higher education as
12 defined by Section 61.003, Education Code, that is created by the
13 constitution or a statute of this state.

14 Sec. 2062.002. CONSENT REQUIRED BEFORE ACQUIRING,
15 RETAINING, OR DISSEMINATING CERTAIN INFORMATION; RECORDS. (a)
16 Except as provided by Subsection (b), a state agency may not:

17 (1) use global positioning system technology,
18 individual contact tracing, or technology designed to obtain
19 biometric identifiers to acquire information that alone or in
20 conjunction with other information identifies an individual or the
21 individual's location without the individual's written or
22 electronic consent;

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

26 (3) disseminate to a person the information described
27 by Subdivision (1) with respect to an individual unless the state

1 agency first obtains the individual's written or electronic
2 consent.

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

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

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

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

15 SECTION 11. (a) Not later than December 1, 2021, the
16 Department of Information Resources shall:

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

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

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

27 (b) Each state agency shall ensure that:

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

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

7 (c) Each state agency subject to Section 2054.137,
8 Government Code, as added by this Act, shall designate a data
9 management officer as soon as practicable after the effective date
10 of this Act.

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

15 SECTION 12. Not later than October 15, 2022, the Department
16 of Information Resources shall submit to the standing committees of
17 the senate and house of representatives with primary jurisdiction
18 over state agency cybersecurity a report on the department's
19 activities and recommendations related to the Texas volunteer
20 incident response team established as required by Subchapter N-2,
21 Chapter 2054, Government Code, as added by this Act.

22 SECTION 13. Chapter 2062, Government Code, as added by this
23 Act, applies only to information acquired, retained, or
24 disseminated by a state agency to another person on or after the
25 effective date of this Act.

26 SECTION 14. (a) Except as provided by Subsection (b) of
27 this section, this Act takes effect immediately if it receives a

1 vote of two-thirds of all the members elected to each house, as
2 provided by Section 39, Article III, Texas Constitution. If this
3 Act does not receive the vote necessary for immediate effect, this
4 Act takes effect September 1, 2021.

5 (b) Chapter 2062, Government Code, as added by this Act,
6 takes effect September 1, 2021.