By: Nelson S.B. No. 475

A BILL TO BE ENTITLED

AN ACT

relating to state agency and local government information 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 C, Chapter 2054, Government Code, is amended by adding Sections 2054.0593 and 2054.05935 to read as follows:

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

(b) The department shall 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.

(c) The department shall prescribe:

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

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

(d) A state agency shall 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. The department shall evaluate vendors to determine whether a vendor qualifies for a certification issued by the department reflecting compliance with program requirements.

(e) A state agency may not enter or renew a contract with a vendor to purchase cloud computing services subject to the state risk and authorization management program unless the vendor demonstrates compliance with program requirements. The vendor may demonstrate compliance by submitting documentation that shows the vendor's compliance with the risk and authorization management program of another state that the department approves.

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

Sec. 2054.05935. SECURITY CONTROLS FOR STATE AGENCY DATA. Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall 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 vendor must periodically provide to the agency evidence that the vendor meets the security controls required under the contract.

SECTION 2. Section 2054.0594, Government Code, is amended by adding Subsection (d) to read as follows:

(d) The department shall 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. A working group may be established within the geographic area of a regional planning commission established under Chapter 391, Local Government Code. The working group may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity event and recovery from the event.

SECTION 3. Subchapter F, Chapter 2054, Government Code, is amended by adding Section 2054.137 to read as follows:

Sec. 2054.137. DESIGNATED DATA MANAGEMENT OFFICER. (a) Each state agency with more than 150 full-time employees shall designate a full-time employee of the agency to serve as a data management officer.

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

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

(2) in accordance with department 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 records management programs are implemented by the agency for all types of data storage media; and

(C) increase awareness of and outreach for state agency records management programs.

(c) In accordance with department guidelines, the data management officer for the state agency shall post on the Texas Open Data Portal established by the department under Section 2054.070 at least three high-value data sets as defined by Section 2054.1265. The high-value data sets may not include information that is confidential or protected from disclosure under state or federal law.

SECTION 4. Subchapter G, Chapter 2054, Government Code, is amended by adding Section 2054.161 to read as follows:

Sec. 2054.161. DATA CLASSIFICATION, SECURITY, AND RETENTION REQUIREMENTS. On initiation of an information resources technology project, including an application development project and any information resources projects described in this subchapter, a state agency shall classify the data produced from or used in the project and determine appropriate data security and retention requirements for each classification.

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

SUBCHAPTER N-2. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2054.52001. DEFINITIONS. In this subchapter:

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

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

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

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

(b) The department shall 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. The department shall enter into a contract with each volunteer the department approves to provide rapid response assistance under this subchapter. The contract must require the volunteer to:

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

(2) protect all confidential information from

disclosure;

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

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

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

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

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

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

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

Sec. 2054.52005. DEPLOYMENT. (a) 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, the department on request of a participating entity may deploy volunteers and provide rapid response assistance under the department's direction to assist with the event.

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

Sec. 2054.52006. CYBERSECURITY COUNCIL DUTIES. The

cybersecurity council established under Section 2054.512 shall review and make recommendations to the department regarding the policies and procedures used by the department to implement this subchapter. The department may consult with the council to implement and administer this subchapter.

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

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

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

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

(A) standards and procedures the department 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) The department may require a participating entity to enter into a contract as a condition for obtaining assistance from the incident response team. The contract must comply with the

requirements of Chapters 771 and 791.

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

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

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

Sec. 2054.52008. STATUS OF VOLUNTEER; LIABILITY. (a) 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) 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. 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. This immunity is limited to services provided during the time of deployment for a cybersecurity event.

Sec. 2054.52010. CONFIDENTIAL INFORMATION. Information written, produced, collected, assembled, or maintained by the department, 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 if the information:

(1) contains the contact information for a volunteer;

(2) 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;

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

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

SECTION 6. Section 2054.515, Government Code, is amended to read as follows:

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

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

(2) data governance program in accordance with requirements established by department rule.

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

(1) the department; and

(2) on request, the governor, the lieutenant governor,

and the speaker of the house of representatives.

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

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

SECTION 7. Chapter 2059, Government Code, is amended by adding Subchapter E to read as follows:

SUBCHAPTER E. REGIONAL NETWORK SECURITY CENTERS

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

Sec. 2059.202. ESTABLISHMENT OF REGIONAL NETWORK SECURITY CENTERS. (a) Subject to Subsection (b), the department may establish regional network security centers 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) The department may establish more than one regional network security center only if the department determines the first center established by the department successfully provides to state

agencies and other eligible entities the services the center has contracted to provide.

(c) The department shall 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) In creating and operating a regional network security center, the department shall partner with a university system or institution of higher education as defined by Section 61.003, Education Code, other than a public junior college. The system or institution shall:

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

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

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

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

(d) A local law enforcement entity or any entity providing

security for a regional network security center shall monitor security alarms at the regional network security center subject to the availability of that service.

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

Sec. 2059.204. REGIONAL NETWORK SECURITY CENTERS SERVICES AND SUPPORT. The department may 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) The department shall 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) The department shall revise the standard operating procedures as necessary to confirm network security.

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

SECTION 8. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2062 to read as follows:

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

Sec. 2062.001. DEFINITIONS. In this chapter:

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

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

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

(1) use 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 consent;

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

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

(b) A state agency may acquire, retain, and disseminate information described by Subsection (a) with respect to an individual without the individual's written 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) A state agency shall retain the written 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 9. (a) Not later than December 1, 2021, the Department of Information Resources shall:

(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) Each state agency shall 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 2054.05935, Government Code, as added by this Act, that is executed on or after the effective date of this Act complies with that section.

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

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

SECTION 10. Not later than October 15, 2022, the Department of Information Resources shall submit to the standing committees of the senate and house of representatives with primary jurisdiction over state agency cybersecurity a report on the department'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 11. Chapter 2062, Government Code, as added by this Act, applies only to information acquired, retained, or disseminated by a state agency to another person on or after the effective date of this Act.

SECTION 12. (a) Except as provided by Subsection (b) of this section, this Act takes effect immediately if it receives a vote of two-thirds of all the members elected to each house, as provided by Section 39, Article III, Texas Constitution. If this Act does not receive the vote necessary for immediate effect, this Act takes effect September 1, 2021.

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