By: Nelson S.B. No. 64

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for information resources.

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

SECTION 1. Subchapter C, Chapter 61, Education Code, is amended by adding Section 61.09091 to read as follows:

Sec. 61.09091. STRATEGIES TO INCENTIVIZE CYBERSECURITY DEGREE PROGRAMS. (a) The board in collaboration with the Department of Information Resources shall identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity.

(b) The board shall consult with institutions of higher education as necessary to carry out its duties under this section.

(c) Not later than September 1, 2020, the board shall submit a written report detailing the strategies identified under this section to the lieutenant governor, the speaker of the house of representatives, the presiding officer of each legislative standing committee with primary jurisdiction over higher education, and each governing board of an institution of higher education.

(d) This section expires September 1, 2021.

SECTION 2. Section 418.004(1), Government Code, is amended to read as follows:

(1) "Disaster" means the occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property

resulting from any natural or man-made cause, including fire, flood, earthquake, wind, storm, wave action, oil spill or other water contamination, volcanic activity, epidemic, air contamination, blight, drought, infestation, explosion, riot, hostile military or paramilitary action, extreme heat, cybersecurity event, other public calamity requiring emergency action, or energy emergency.

SECTION 3. Section 815.103, Government Code, is amended by adding Subsection (g) to read as follows:

(g) The retirement system shall comply with cybersecurity and information security standards established by the Department of Information Resources under Chapter 2054.

SECTION 4. Section 825.103, Government Code, is amended by amending Subsection (e) and adding Subsection (e-1) to read as follows:

(e) Except as provided by Subsection (e-1), Chapters 2054 and 2055 do not apply to the retirement system. The board of trustees shall control all aspects of information technology and associated resources relating to the retirement system, including computer, data management, and telecommunication operations, procurement of hardware, software, and middleware, and telecommunication equipment and systems, location, operation, and replacement of computers, computer systems, and telecommunication systems, data processing, security, disaster recovery, and storage. The Department of Information Resources shall assist the retirement system at the request of the retirement system, and the retirement system may use any service that is available through that department.

<u>(e-1) The retirement system shall comply with cybersecurity and information security standards established by the Department of Information Resources under Chapter 2054.</u>

SECTION 5. Section 2054.0075, Government Code, is amended to read as follows:

Sec. 2054.0075. EXCEPTION: PUBLIC JUNIOR COLLEGE. This chapter does not apply to a public junior college or a public junior college district, except as necessary <u>to comply with information security standards and</u> for participation in <u>shared technology services, including</u> the electronic government project implemented under Subchapter I and <u>statewide technology centers under Subchapter L</u> [~~except as to Section 2054.119, Government Code~~].

SECTION 6. Section 2054.0591(a), Government Code, is amended to read as follows:

(a) Not later than November 15 of each even-numbered year, the department shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity event;

(2) a review of existing statutes regarding cybersecurity and information resources technologies;

(3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity event; and

(4) an evaluation of a program that provides an information security officer to assist small state agencies and local governments that are unable to justify hiring a full-time information security officer [~~the costs and benefits of cybersecurity insurance; and~~

[~~(5) an evaluation of tertiary disaster recovery options~~].

SECTION 7. Section 2054.0594, Government Code, is amended to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS ORGANIZATION [~~CENTER~~]. (a) The department shall establish an information sharing and analysis organization [~~center~~] to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) [~~The department shall appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.~~

[~~(c)~~] The department[~~, using funds other than funds appropriated to the department in a general appropriations act,~~] shall provide administrative support to the information sharing and analysis organization [~~center~~].

(c) A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information shared through the organization. Section 552.007 does not apply to information described by this subsection.

SECTION 8. Section 2054.068(e), Government Code, is amended to read as follows:

(e) The consolidated report required by Subsection (d) must:

(1) include an analysis and assessment of each state agency's security and operational risks; and

(2) for a state agency found to be at higher security and operational risks, include a detailed analysis of agency efforts to address the risks and related vulnerabilities[~~, and an estimate of the costs to implement, the:~~

[~~(A) requirements for the agency to address the risks and related vulnerabilities; and~~

[~~(B) agency's efforts to address the risks through the:~~

[~~(i) modernization of information technology systems;~~

[~~(ii) use of cloud services; and~~

[~~(iii) use of a statewide technology center established by the department~~].

SECTION 9. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.069 to read as follows:

Sec. 2054.069. PRIORITIZED CYBERSECURITY AND LEGACY SYSTEM

PROJECTS REPORT. (a) Not later than October 1 of each even-numbered year, the department shall submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency:

(1) cybersecurity projects; and

(2) projects to modernize or replace legacy systems, as defined by Section 2054.571.

(b) Each state agency shall coordinate with the department to implement this section.

(c) A state agency shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information contained in or written, produced, collected, assembled, or maintained in connection with the report under Subsection (a). Section 552.007 does not apply to information described by this subsection.

SECTION 10. Sections 2054.077(b) and (d), Government Code, are amended to read as follows:

(b) The information security officer [~~resources manager~~] of a state agency shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(d) The information security officer [~~resources manager~~] shall provide an electronic copy of the vulnerability report on its completion to:

(1) the department;

(2) the state auditor;

(3) the agency's executive director;

(4) the agency's designated information resources manager; and

(5) [~~(4)~~] any other information technology security oversight group specifically authorized by the legislature to receive the report.

SECTION 11. Section 2054.1125, Government Code, is amended by amending Subsection (b) and adding Subsection (c) to read as follows:

(b) A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

(A) the department, including the chief

information security officer [~~and the state cybersecurity coordinator~~]; or

(B) if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

(c) Not later than the 10th business day after the date of the eradication, closure, and recovery from a breach, suspected breach, or unauthorized exposure, a state agency shall notify the department, including the chief information security officer, of the details of the event.

SECTION 12. Section 2054.133(e), Government Code, is amended to read as follows:

(e) Each state agency shall include in the agency's information security plan a written document that is signed by [~~acknowledgment that~~] the [~~executive director or other~~] head of the agency, the chief financial officer, and each executive manager [~~as~~] designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan.

SECTION 13. Section 2054.516, Government Code, as added by Chapters 683 (H.B. 8) and 955 (S.B. 1910), Acts of the 85th Legislature, Regular Session, 2017, is reenacted and amended to read as follows:

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency[~~, other than an institution of higher education subject to Section 2054.517,~~] implementing an Internet website or mobile application that processes any sensitive personal <u>or</u> personally identifiable information or confidential information must:

(1) submit a biennial data security plan to the department not later than October 15 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

(b) The department shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after the department reviews the plan.

SECTION 14. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Section 2054.519 to read as follows:

<u>Sec. 2054.519. APPLICABILITY OF LAW TO CERTAIN ORGANIZATIONS. For the purposes of a provision relating to cybersecurity under this chapter, an independent organization certified under Section 39.151, Utilities Code, is considered to be a state agency.</u>

SECTION 15. Section 2059.058(b), Government Code, is amended to read as follows:

(b) In addition to the department's duty to provide network security services to state agencies under this chapter, the department by agreement may provide network security to:

(1) each house of the legislature;

(2) an agency that is not a state agency, including a legislative agency;

(3) a political subdivision of this state, including a county, municipality, or special district; [~~and~~]

(4) an independent organization, as defined by Section 39.151, Utilities Code; and

(5) a public junior college.

SECTION 16. Section 1702.104, Occupations Code, is amended by adding Subsection (c) to read as follows:

(c) The review and analysis of computer-based data for the purpose of preparing for or responding to a cybersecurity event does not constitute an investigation for purposes of this section and does not require licensing under this chapter.

SECTION 17. Chapter 31, Utilities Code, is amended by designating Sections 31.001 through 31.005 as Subchapter A and adding a subchapter heading to read as follows:

SUBCHAPTER A. GENERAL PROVISIONS

SECTION 18. Chapter 31, Utilities Code, is amended by adding Subchapter B to read as follows:

SUBCHAPTER B. CYBERSECURITY

Sec. 31.051. DEFINITION. In this subchapter, "utility" means:

(1) an electric cooperative;

(2) an electric utility;

(3) a municipally owned electric utility;

(4) a power marketer;

(5) a retail electric provider; or

(6) a transmission and distribution utility.

Sec. 31.052. CYBERSECURITY COORDINATION PROGRAM FOR

UTILITIES. (a) The commission shall establish a program to coordinate cybersecurity efforts among utilities in this state. The program shall provide guidance on best practices in cybersecurity and facilitate the sharing of cybersecurity information between utilities.

(b) The commission may collaborate with the state cybersecurity coordinator and the cybersecurity council established under Chapter 2054, Government Code, in implementing the program.

Sec. 31.053. APPROVED CYBERSECURITY VENDOR LIST. (a) The commission shall create and periodically update a list of approved vendors of information technology providers.

(b) A utility may not enter into a contract with an information technology provider that is not an approved vendor on the list created under this section.

(c) A contract that does not comply with Subsection (b) is void and unenforceable.

(d) In creating and updating the list and criteria used for the list, the commission shall consider:

(1) contracting guidelines set by the United States Department of Defense for information technology providers; and

(2) cybersecurity best practices developed by the National Institute of Standards and Technology and the Center for Internet Security.

(e) The commission shall publish the criteria used to create the list.

SECTION 19. (a) Sections 2054.119 and 2054.517, Government

Code, are repealed.

(b) Section 17, Chapter 683 (H.B. 8), Acts of the 85th Legislature, Regular Session, 2017, is repealed.

SECTION 20. An independent organization certified under Section 39.151, Utilities Code, shall enter into a memorandum of understanding with the Department of Information Resources relating to the independent organization's compliance with cybersecurity provisions administered by the department under Chapter 2054, Government Code, for state agencies consistent with Section 2054.519, Government Code, as added by this Act. The memorandum of understanding must include a timetable for the independent organization's compliance not later than January 31, 2020, with the department's cybersecurity regulations.

SECTION 21. The Public Utility Commission of Texas shall create the vendor list required by Section 31.053, Utilities Code, as added by this Act, not later than December 31, 2019.

SECTION 22. The changes in law made by Section 31.053, Utilities Code, as added by this Act, apply only to a contract entered into on or after December 31, 2019. A contract entered into before that date is governed by the law in effect immediately before the effective date of this Act, and the former law is continued in effect for that purpose.

SECTION 23. To the extent of any conflict, this Act prevails over another Act of the 86th Legislature, Regular Session, 2019, relating to nonsubstantive additions and corrections in enacted codes.

SECTION 24. This Act takes effect September 1, 2019.