By: Capriglione H.B. No. 8

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for state agency information resources.

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

SECTION 1. This Act may be cited as the Texas Cybersecurity Act.

SECTION 2. Section 325.011, Government Code, is amended to read as follows:

Sec. 325.011. CRITERIA FOR REVIEW. The commission and its staff shall consider the following criteria in determining whether a public need exists for the continuation of a state agency or its advisory committees or for the performance of the functions of the agency or its advisory committees:

(1) the efficiency and effectiveness with which the agency or the advisory committee operates;

(2)(A) an identification of the mission, goals, and objectives intended for the agency or advisory committee and of the problem or need that the agency or advisory committee was intended to address; and

(B) the extent to which the mission, goals, and objectives have been achieved and the problem or need has been addressed;

(3)(A) an identification of any activities of the agency in addition to those granted by statute and of the authority for those activities; and

(B) the extent to which those activities are needed;

(4) an assessment of authority of the agency relating to fees, inspections, enforcement, and penalties;

(5) whether less restrictive or alternative methods of performing any function that the agency performs could adequately protect or provide service to the public;

(6) the extent to which the jurisdiction of the agency and the programs administered by the agency overlap or duplicate those of other agencies, the extent to which the agency coordinates with those agencies, and the extent to which the programs administered by the agency can be consolidated with the programs of other state agencies;

(7) the promptness and effectiveness with which the agency addresses complaints concerning entities or other persons affected by the agency, including an assessment of the agency's administrative hearings process;

(8) an assessment of the agency's rulemaking process and the extent to which the agency has encouraged participation by the public in making its rules and decisions and the extent to which the public participation has resulted in rules that benefit the public;

(9) the extent to which the agency has complied with:

(A) federal and state laws and applicable rules regarding equality of employment opportunity and the rights and privacy of individuals; and

(B) state law and applicable rules of any state

agency regarding purchasing guidelines and programs for historically underutilized businesses;

(10) the extent to which the agency issues and enforces rules relating to potential conflicts of interest of its employees;

(11) the extent to which the agency complies with Chapters 551 and 552 and follows records management practices that enable the agency to respond efficiently to requests for public information;

(12) the effect of federal intervention or loss of federal funds if the agency is abolished; [~~and~~]

(13) the extent to which the purpose and effectiveness of reporting requirements imposed on the agency justifies the continuation of the requirement; and

(14) an assessment of the agency's cybersecurity practices.

SECTION 3. Subchapter A, Chapter 411, Government Code, is amended by adding Section 411.00431 to read as follows:

Sec. 411.00431. CYBERSECURITY RISKS AND INCIDENTS. (a) The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in addressing cybersecurity risks and incidents in this state. The agreement may include provisions for:

(1) providing training to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents;

(2) developing and maintaining a cybersecurity risks and incidents curriculum using existing programs and models for training state and local officials and first responders;

(3) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(4) conducting cybersecurity training and simulation exercises for state agencies, political subdivisions, and private entities to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(5) assisting state agencies and political subdivisions in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

(6) incorporating cybersecurity risk and incident prevention and response methods into existing state and local emergency plans, including continuity of operation plans and incident response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the department shall seek to prevent unnecessary duplication of existing programs or efforts of the department or another state agency.

(c) In selecting an organization under Subsection (a), the department shall consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

(d) The department shall consult with institutions of

higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 4. Subchapter B, Chapter 421, Government Code, is amended by adding Section 421.027 to read as follows:

Sec. 421.027. CYBER ATTACK STUDY AND RESPONSE PLAN. (a) In this section, "cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

(b) The council shall:

(1) conduct a study regarding cyber attacks on state agencies and on critical infrastructure that is owned, operated, or controlled by agencies; and

(2) develop a state response plan to be implemented by an agency in the event of a cyber attack on the agency or on critical infrastructure that is owned, operated, or controlled by the agency.

(c) Not later than September 1, 2018, the council shall deliver the response plan and a report on the findings of the study to:

(1) the public safety director of the Department of Public Safety;

(2) the governor;

(3) the lieutenant governor;

(4) the speaker of the house of representatives;

(5) the chair of the committee of the senate having primary jurisdiction over homeland security matters; and

(6) the chair of the committee of the house of representatives having primary jurisdiction over homeland security matters.

(d) The response plan required by Subsection (b) and the report required by Subsection (c) are not public information for purposes of Chapter 552.

(e) This section expires December 1, 2018.

SECTION 5. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0593 to read as follows:

Sec. 2054.0593. CYBERSECURITY TASK FORCE. (a) The department shall establish and lead a cybersecurity task force to engage members of the task force in policy discussions and educate state agencies on cybersecurity issues. The department shall determine the composition of the task force, which may include representatives of state agencies and other interested parties.

(b) The task force shall:

(1) consolidate and synthesize existing cybersecurity resources and best practices to assist state agencies in understanding and implementing cybersecurity measures that are most beneficial to this state;

(2) develop reliable, clear, and concise guidelines on cyber threat detection and prevention, including best practices and remediation strategies for state agencies;

(3) develop state agency guidelines for easily replicated cybersecurity initiatives;

(4) provide opportunities for state agency technology leaders and members of the legislature to participate in programs

and webinars on critical cybersecurity policy issues; and

(5) provide recommendations to the legislature on any needed legislation to implement cybersecurity best practices and remediation strategies for state agencies.

(c) The task force is abolished September 1, 2019, unless the department extends the task force until September 1, 2021.

(d) This section expires September 1, 2021.

SECTION 6. Section 2054.076, Government Code, is amended by adding Subsection (b-1) to read as follows:

(b-1) The department shall provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training and certification that must be completed by all information resources employees of the agencies.

SECTION 7. Section 2054.1125(b), Government Code, is amended 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[~~, in the event of a breach of system security,~~] 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) notify the department, including the chief information security officer and the state cybersecurity coordinator, not later than 48 hours after the discovery of the

breach, suspected breach, or unauthorized exposure.

SECTION 8. Section 2054.133, Government Code, is amended by adding Subsections (b-1), (b-2), and (b-3) to read as follows:

(b-1) The executive head and chief information security officer of each state agency shall annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches.

(b-2) Before submitting to the Legislative Budget Board a legislative appropriation request for a state fiscal biennium, a state agency must file with the board the written approval required under Subsection (b-1) for each year of the current state fiscal biennium.

(b-3) Each state agency shall include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. The agency shall, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The agency may incorporate the core functions over a period of years.

SECTION 9. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.515, 2054.516, and 2054.517 to read as follows:

Sec. 2054.515. INDEPENDENT RISK ASSESSMENT. (a) At least once every five years, in accordance with department rules, each state agency shall:

(1) contract with an independent third party selected from a list provided by the department to conduct an independent risk assessment of the agency's exposure to security risks in the agency's information resources systems; and

(2) submit the results of the independent risk assessment to the department.

(b) The department shall submit to the legislature a comprehensive report on the results of the independent risk assessments conducted under Subsection (a) that identifies systematic or pervasive security risk vulnerabilities across state agencies and recommendations for addressing the vulnerabilities.

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency implementing an Internet website or mobile application that processes any personally identifiable or confidential information must:

(1) submit a data security plan to the department before beta testing the website or application; and

(2) before deploying the website or application:

(A) subject the website or application to a vulnerability and penetration test conducted by an independent third party; and

(B) address any vulnerability identified under Paragraph (A).

(b) The data security plan required under Subsection (a)(1)

must include:

(1) data flow diagrams to show the location of information in use, in transit, and not in use;

(2) data storage locations;

(3) data interaction with online or mobile devices;

(4) security of data transfer;

(5) security measures for the online or mobile application; and

(6) a description of any action taken by the agency to remediate any vulnerability identified by an independent third party under Subsection (a)(2).

(c) 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.

Sec. 2054.517. VENDOR RESPONSIBILITY FOR CYBERSECURITY. A vendor that contracts with the state to provide information resources technology for a state agency is responsible for addressing known cybersecurity risks associated with the technology and any costs associated with addressing the identified cybersecurity risks.

SECTION 10. Section 2054.575(a), Government Code, is amended to read as follows:

(a) A state agency shall, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. The agency shall include in the plan:

(1) procedures for reducing the agency's level of exposure with regard to information that alone or in conjunction with other information identifies an individual maintained on a legacy system of the agency; and

(2) the most cost-effective approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities.

SECTION 11. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2061 to read as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITION. In this chapter, "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. 2061.002. DESTRUCTION AUTHORIZED. (a) A state agency shall destroy or arrange for the destruction of information that alone or in conjunction with other information identifies an individual if the agency is not required to retain the information under other law.

(b) A state agency shall destroy or arrange for the destruction of information described by Subsection (a) by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive information in the records to make the information unreadable or indecipherable

through any means.

SECTION 12. Section 2157.007, Government Code, is amended by adding Subsection (e) to read as follows:

(e) The department shall periodically review guidelines on state agency information that may be stored by a cloud computing service and the cloud computing systems available to state agencies for that storage to ensure that an agency purchasing a major information resources project under Section 2054.118 selects the most affordable, secure, and efficient cloud computing service available to the agency.

SECTION 13. Chapter 276, Election Code, is amended by adding Section 276.011 to read as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the Texas Rangers shall conduct a study regarding cyber attacks on election infrastructure and shall report its findings to the standing committees of the legislature with jurisdiction over election procedures. The study shall include:

(1) an investigation of vulnerabilities and risks for a cyber attack against a county's voting system machines or the list of registered voters;

(2) information on any attempted cyber attack on a county's voting system machines or the list of registered voters; and

(3) recommendations for protecting a county's voting system machines and list of registered voters from a cyber attack.

(b) This section expires January 1, 2019.

SECTION 14. (a) The lieutenant governor shall establish a

Senate Select Committee on Cybersecurity and the speaker of the house of representatives shall establish a House Select Committee on Cybersecurity to, jointly or separately, study:

(1) cybersecurity in this state;

(2) the information security plans of each state agency; and

(3) the risks and vulnerabilities of state agency cybersecurity.

(b) Not later than November 30, 2017:

(1) the lieutenant governor shall appoint five senators to the Senate Select Committee on Cybersecurity, one of whom shall be designated as chair; and

(2) the speaker of the house of representatives shall appoint five state representatives to the House Select Committee on Cybersecurity, one of whom shall be designated as chair.

(c) The committees established under this section shall convene separately at the call of the chair of the respective committees, or jointly at the call of both chairs. In joint meetings, the chairs of each committee shall act as joint chairs.

(d) Following consideration of the issues listed in Subsection (a) of this section, the committees established under this section shall jointly adopt recommendations on state cybersecurity and report in writing to the legislature any findings and adopted recommendations not later than January 13, 2019.

(e) This section expires September 1, 2019.

SECTION 15. (a) In this section, "state agency" means a board, commission, office, department, council, authority, or

other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state. The term does not include a university system or institution of higher education as those terms are defined by Section 61.003, Education Code.

(b) The Department of Information Resources and the Texas State Library and Archives Commission shall conduct a study on state agency digital data storage and records management practices and the associated costs to this state.

(c) The study required under this section must examine:

(1) the current digital data storage practices of state agencies in this state;

(2) the costs associated with those digital data storage practices;

(3) the digital records management and data classification policies of state agencies and whether the state agencies are consistently complying with the established policies;

(4) whether the state agencies are storing digital data that exceeds established retention requirements and the cost of that unnecessary storage;

(5) the adequacy of storage systems used by state agencies to securely maintain confidential digital records; and

(6) possible solutions and improvements recommended by the state agencies for reducing state costs and increasing security for digital data storage and records management.

(d) Each state agency shall participate in the study required by this section and provide appropriate assistance and

information to the Department of Information Resources and the Texas State Library and Archives Commission.

(e) Not later than December 1, 2018, the Department of Information Resources and the Texas State Library and Archives Commission shall issue a report on the study required under this section and recommendations for reducing state costs and for improving efficiency in digital data storage and records management to the lieutenant governor, the speaker of the house of representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) This section expires September 1, 2019.

SECTION 16. The changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 17. This Act takes effect September 1, 2017.