By: Capriglione H.B. No. 3892

A BILL TO BE ENTITLED

AN ACT

relating to matters concerning governmental entities, including cybersecurity, governmental efficiencies, information resources, and emergency planning.

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

SECTION 1. Section 37.108(b), Education Code, is amended to read as follows:

(b) At least once every three years, each school district or public junior college district shall conduct a safety and security audit of the district's facilities, including an information technology cybersecurity assessment. To the extent possible, a district shall follow safety and security audit procedures developed by the Texas School Safety Center or a person included in the registry established by the Texas School Safety Center under Section 37.2091.

SECTION 2. Subchapter A, Chapter 31, Election Code, is amended by adding Section 31.017 to read as follows:

Sec. 31.017. STUDY ON USE OF ARTIFICIAL INTELLIGENCE FOR SIGNATURE VERIFICATION. (a) The secretary of state shall conduct a study on the use of artificial intelligence to verify signatures on carrier envelope certificates for early voting ballots voted by mail. In conducting the study, the secretary of state must consider other states' experiences using that method of signature verification, as well as other studies published on the subject.

(b) Not later than September 1, 2022, the secretary of state shall prepare and deliver a report on the study's findings to the committees of each house of the legislature with primary jurisdiction over elections.

(c) This section expires December 1, 2022.

SECTION 3. Subchapter B, Chapter 421, Government Code, is amended by adding Section 421.027 to read as follows:

Sec. 421.027. CYBER INCIDENT STUDY AND RESPONSE PLAN. (a) In this section:

(1) "Cyber incident" means an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information on the computers or systems. The term includes a vulnerability in implementation or in an information system, system security procedure, or internal control that could be exploited by a threat source.

(2) "Significant cyber incident" means a cyber incident, or a group of related cyber incidents, likely to result in demonstrable harm to state security interests, foreign relations, or the economy of this state or to the public confidence, civil liberties, or public health and safety of the residents of this state.

(b) The council, in cooperation with the Department of Information Resources, shall:

(1) conduct a study regarding cyber incidents and

significant cyber incidents affecting state agencies and critical infrastructure that is owned, operated, or controlled by agencies; and

(2) develop a comprehensive state response plan to provide a format for each state agency to develop an agency-specific response plan and to implement the plan into the agency's information security plan required under Section 2054.133 to be implemented by the agency in the event of a cyber incident or significant cyber incident affecting the agency or critical infrastructure that is owned, operated, or controlled by the agency.

(c) Not later than September 1, 2022, 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, 2022.

SECTION 4. Subchapter L, Chapter 441, Government Code, is amended by adding Sections 441.1825 and 441.1856 to read as follows:

Sec. 441.1825. STATE INFORMATION GOVERNANCE COORDINATOR. (a) The director and librarian shall employ a state information governance coordinator in the commission's records management division.

(b) The state information governance coordinator shall:

(1) ensure records management programs are implemented by state agencies for all media types;

(2) assist state agencies in complying with the agencies' records management programs; and

(3) increase overall awareness and outreach for state agency records management programs.

Sec. 441.1856. TEXAS DIGITAL ARCHIVE. (a) The commission shall maintain and operate a digital repository for the preservation of and access to permanently valuable archival state records, reports, and publications.

(b) The commission, in collaboration with the Department of Information Resources, shall develop a strategy, consistent with state records management and archival practices, for state agencies to transfer appropriate archival state records that are in electronic format to the commission for inclusion in the digital repository described by Subsection (a).

SECTION 5. Section 441.183, Government Code, is amended to read as follows:

Sec. 441.183. RECORDS MANAGEMENT PROGRAMS IN STATE AGENCIES. (a) The agency head of each state agency shall:

(1) establish and maintain a records management program on a continuing and active basis;

(2) create and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the financial and legal rights of the state and any person affected by the activities of the agency;

(3) make certain that all records of the agency are passed to the agency head's successor in the position of agency head;

(4) identify and take adequate steps to protect confidential and vital state records;

(5) cooperate with the commission in the conduct of state agency records management surveys; and

(6) cooperate with the commission, the director and librarian, and any other authorized designee of the director and librarian in fulfilling their duties under this subchapter.

(b) This subsection applies only to a state agency that is a department, commission, board, office, or other agency in the executive branch of state government. This subsection does not apply to an institution of higher education, as defined by Section 61.003, Education Code. As part of a records management program established under Subsection (a), the agency head of a state agency to which this subsection applies shall require training for agency employees, annually and on employment with the agency, regarding the records management program, including the agency's approved records retention schedule.

SECTION 6. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0695 to read as follows:

Sec. 2054.0695. SECURITY PROGRAM FOR INTERNET CONNECTIVITY OF CERTAIN OBJECTS. (a) The department, in consultation with representatives of the information technology industry and voluntary standards organizations and the 10 state agencies that received the most state appropriations for that state fiscal year as determined by the Legislative Budget Board, shall develop a comprehensive risk management program that identifies baseline security features for the Internet connectivity of computing devices embedded in objects used or purchased by state agencies.

(b) In developing the program under Subsection (a), the department shall identify and use existing international security standards and best practices and any known security gaps for a range of deployments, including critical systems and consumer usage.

SECTION 7. Section 2054.512(d), Government Code, is amended to read as follows:

(d) The cybersecurity council shall:

(1) consider the costs and benefits of establishing a computer emergency readiness team to address cyber attacks occurring in this state during routine and emergency situations;

(2) establish criteria and priorities for addressing cybersecurity threats to critical state installations;

(3) consolidate and synthesize best practices to

assist state agencies in understanding and implementing cybersecurity measures that are most beneficial to this state; [~~and~~]

(4) assess the knowledge, skills, and capabilities of the existing information technology and cybersecurity workforce to mitigate and respond to cyber threats and develop recommendations for addressing immediate workforce deficiencies and ensuring a long-term pool of qualified applicants; and

(5) ensure all middle and high schools have knowledge of and access to:

(A) free cybersecurity courses and curriculum approved by the Texas Education Agency;

(B) state and regional information sharing and analysis centers; and

(C) contracting benefits, including as provided by Section 2054.0565.

SECTION 8. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.517 and 2054.5172 to read as follows:

Sec. 2054.517. VENDOR RESPONSIBILITY FOR CYBERSECURITY. A vendor that contracts with this state to provide information resources technology for a state agency at a cost to the agency of $1 million or more is responsible for addressing known cybersecurity risks associated with the technology and is responsible for any cost associated with addressing the identified cybersecurity risks. For a major information resources project, the vendor shall provide to state agency contracting personnel:

(1) a written attestation that:

(A) the vendor has a cybersecurity risk management program consistent with:

(i) the cybersecurity framework established by the National Institute of Standards and Technology;

(ii) the 27000 series standards for information security published by the International Organization for Standardization; or

(iii) other widely accepted security risk management frameworks;

(B) the vendor's cybersecurity risk management program includes appropriate training and certifications for the employees performing work under the contract; and

(C) the vendor has a vulnerability management program that addresses vulnerability identification, mitigation, and responsible disclosure, as appropriate; and

(2) an initial summary of any costs associated with addressing or remediating the identified technology or personnel-related cybersecurity risks as identified in collaboration with this state following a risk assessment.

Sec. 2054.5172. ENCRYPTED SECURE LAYER SERVICES REQUIRED. Each state agency that maintains a publicly accessible Internet website that requires the submission of sensitive personally identifiable information shall use an encrypted secure communication protocol, including a secure hypertext transfer protocol.

SECTION 9. Subchapter B, Chapter 2155, Government Code, is amended by adding Section 2155.092 to read as follows:

Sec. 2155.092. VENDOR CERTIFICATION FOR CERTAIN GOODS. (a) This section does not apply to a good provided as part of a major information resources project as defined by Section 2054.003.

(b) A vendor offering to sell to the state a good embedded with a computing device capable of Internet connectivity must include with each bid, offer, proposal, or other expression of interest a written certification providing that the good does not contain, at the time of submitting the bid, offer, proposal, or expression of interest, a hardware, software, or firmware component with any known security vulnerability or defect.

SECTION 10. Section 205.010(b), Local Government Code, is amended to read as follows:

(b) A local government that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply, in the event of a breach of system security, with the notification requirements of:

(1) Sections 364.0051 and 364.0102 of this code; and

(2) Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state.

SECTION 11. Subtitle C, Title 11, Local Government Code, is amended by adding Chapter 364 to read as follows:

CHAPTER 364. LOCAL GOVERNMENT CYBERSECURITY AND EMERGENCY PLANNING AND RESPONSE

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 364.0001. DEFINITIONS. In this chapter:

(1) "Breach of system security" has the meaning

assigned by Section 521.053, Business & Commerce Code.

(2) "Cybersecurity coordinator" means the state cybersecurity coordinator designated under Section 2054.511, Government Code.

(3) "Cybersecurity council" means the council established by the cybersecurity coordinator under Section 2054.512, Government Code.

(4) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.

SUBCHAPTER B. SECURITY BREACH NOTIFICATION

Sec. 364.0051. NOTICE TO CYBERSECURITY COORDINATOR. Not later than 48 hours after a political subdivision discovers a breach or suspected breach of system security or an unauthorized exposure of sensitive personal information, the political subdivision shall notify the cybersecurity coordinator of the breach. The notification must describe the breach, suspected breach, or unauthorized exposure.

Sec. 364.0052. REPORT TO DEPARTMENT OF INFORMATION RESOURCES. The cybersecurity coordinator shall report to the Department of Information Resources any breach of system security reported by a political subdivision in which the person responsible for the breach:

(1) obtained or modified specific critical or sensitive personal information;

(2) established access to the political subdivision's information systems or infrastructure; or

(3) undermined, severely disrupted, or destroyed a

core service, program, or function of the political subdivision, or placed the person in a position to do so in the future.

Sec. 364.0053. RULEMAKING. The cybersecurity coordinator may adopt rules necessary to implement this subchapter.

SUBCHAPTER C. EMERGENCY PLANNING AND RESPONSE

Sec. 364.0101. MULTIHAZARD EMERGENCY OPERATIONS PLAN; SAFETY AND SECURITY AUDIT. (a) This section applies to a municipality or county with a population of more than 100,000.

(b) Each municipality and county shall adopt and implement a multihazard emergency operations plan for use in the municipality's and county's facilities. The plan must address mitigation, preparedness, response, and recovery as determined by the cybersecurity council and the governor's public safety office. The plan must provide for:

(1) municipal or county employee training in responding to an emergency;

(2) measures to ensure coordination with the Department of State Health Services, Department of Information Resources, local emergency management agencies, law enforcement agencies, local health departments, and fire departments in the event of an emergency; and

(3) the implementation of a safety and security audit as required by Subsection (c).

(c) At least once every three years, each municipality and county shall conduct a safety and security audit of the municipality's or county's information technology infrastructure. To the extent possible, a municipality or county shall follow safety and security audit procedures developed by the cybersecurity council or a comparable public or private entity.

(d) A municipality or county shall report the results of the safety and security audit conducted under Subsection (c):

(1) to the municipality's or county's governing body; and

(2) in the manner required by the cybersecurity council, to the cybersecurity council.

(e) Except as provided by Subsection (f), any document or information collected, developed, or produced during a safety and security audit conducted under Subsection (c) is not subject to disclosure under Chapter 552, Government Code.

(f) A document relating to a municipality's or county's multihazard emergency operations plan is subject to disclosure if the document enables a person to:

(1) verify that the municipality or county has established a plan and determine the agencies involved in the development of the plan and the agencies coordinating with the municipality or county to respond to an emergency;

(2) verify that the municipality's or county's plan was reviewed within the last 12 months and determine the specific review dates;

(3) verify that the plan addresses the phases of emergency management under Subsection (b);

(4) verify that municipal or county employees have been trained to respond to an emergency and determine the types of training, the number of employees trained, and the person

conducting the training;

(5) verify that the municipality or county has completed a safety and security audit under Subsection (c) and determine the date the audit was conducted, the person conducting the audit, and the date the municipality or county presented the results of the audit to the municipality's or county's governing body; and

(6) verify that the municipality or county has addressed any recommendations by the municipality's or county's governing body for improvement of the plan and determine the municipality's or county's progress within the last 12 months.

Sec. 364.0102. RANSOMWARE PAYMENTS PROHIBITED. (a) In this section, "ransomware" has the meaning assigned by Section 33.023, Penal Code.

(b) A political subdivision may not make a ransomware payment related to a ransomware cyber attack.

(c) As soon as practicable after discovering a ransomware cyber attack, a political subdivision shall report the attack to the office of the attorney general and to the information sharing and analysis organization established by the Department of Information Resources under Sec. 2054.0594, Government Code.

SECTION 12. Section 2155.092, Government Code, as added by this Act, applies only in relation to a contract for which a state agency first advertises or otherwise solicits bids, offers, proposals, or other expressions of interest on or after the effective date of this Act.

SECTION 13. (a) Except as provided by Subsection (b) of this section, this Act takes effect September 1, 2021.

(b) Section 364.0102, Local Government Code, as added by this Act, takes effect September 1, 2022.