By: Capriglione, Bohac, Blanco, Shaheen, Bernal, et al. H.B. No. 4214

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 comparable public or private entity.

SECTION 2. Subchapter C, Chapter 61, Education Code, is amended by adding Section 61.09092 to read as follows:

Sec. 61.09092. COORDINATION OF CYBERSECURITY COURSEWORK DEVELOPMENT. (a) In this section, "lower-division institution of higher education" means a public junior college, public state college, or public technical institute.

(b) The board, in consultation with the Department of Information Resources, shall coordinate with lower-division institutions of higher education and entities that administer or award postsecondary industry certifications or other workforce

credentials in cybersecurity to develop certificate programs or other courses of instruction leading toward those certifications or credentials that may be offered by lower-division institutions of higher education.

(c) The board may adopt rules as necessary for the administration of this section.

SECTION 3. Subchapter F, Chapter 401, Government Code, is amended by adding Section 401.106 to read as follows:

Sec. 401.106. CHIEF INNOVATION OFFICER. (a) The governor shall appoint a chief innovation officer.

(b) The chief innovation officer shall:

(1) develop procedures and processes to improve internal state government efficiency and performance;

(2) develop methods to improve the experience of residents, businesses, and local governments in interacting with state government;

(3) in cooperation with the Department of Information Resources, increase the use of technology by state agencies to improve services provided by the agencies and to reduce state expenses and inefficiencies;

(4) provide state agency personnel with training in skills that support innovation;

(5) provide state agency managers with training to support innovation and encourage creative thinking; and

(6) develop and apply measures to document improvements in state government innovation and in employee skills that support innovation.

(c) In performing the duties required under Subsection (b), the chief innovation officer shall:

(1) use strategic innovation;

(2) promote open innovation;

(3) introduce and use group tools and processes that encourage creative thinking; and

(4) conduct market research to determine the best practices for increasing innovation and implement those best practices.

SECTION 4. 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, cyber attack, other public calamity requiring emergency action, or energy emergency.

SECTION 5. 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 and the Information Technology Council for Higher Education, 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, 2020, 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, 2020.

SECTION 6. Subchapter F, Chapter 437, Government Code, is amended by adding Section 437.255 to read as follows:

Sec. 437.255. ASSISTING TEXAS STATE GUARD WITH CYBER OPERATIONS. To serve the state and safeguard the public from malicious cyber activity, the governor may command the Texas National Guard to assist the Texas State Guard with defending the state's cyber operations.

SECTION 7. Subchapter C, Chapter 531, Government Code, is amended by adding Section 531.1051 to read as follows:

Sec. 531.1051. TECHNOLOGY FOR ELIGIBILITY FRAUD

PREVENTION. (a) The commission shall use technology to identify the risk for fraud associated with applications for health and human services program benefits to prevent fraud with respect to eligibility determinations for those programs. To the extent allowed by federal law, the commission shall set appropriate verification and documentation requirements based on the risk identified for particular applications to ensure that commission resources are appropriately targeted to maximize fraud reduction and accuracy of eligibility determinations.

(b) Enhanced eligibility screening tools the commission implements for the purposes of this section must use technology that provides non-modeled employment and income verification data in an automated electronic format.

SECTION 8. The heading to Section 656.047, Government Code, is amended to read as follows:

Sec. 656.047. PAYMENT OF PROGRAM AND CERTIFICATION EXAMINATION EXPENSES.

SECTION 9. Section 656.047, Government Code, is amended by adding Subsection (a-1) to read as follows:

(a-1) A state agency may spend public funds as appropriate to reimburse a state agency employee or administrator who serves in an information technology, cybersecurity, or other cyber-related position for fees associated with industry-recognized certification examinations.

SECTION 10. Chapter 2051, Government Code, is amended by adding Subchapter E to read as follows:

SUBCHAPTER E. UNIFORM ELECTRONIC LEGAL MATERIAL ACT

Sec. 2051.151. SHORT TITLE. This subchapter may be cited as the Uniform Electronic Legal Material Act.

Sec. 2051.152. DEFINITIONS. In this subchapter:

(1) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(2) "Legal material" means, whether or not in effect:

(A) the constitution of this state;

(B) the general or special laws passed in a regular or special session of the Texas Legislature; and

(C) a state agency rule adopted in accordance with Chapter 2001.

(3) "Official publisher" means:

(A) for legal material described by Subdivision (2)(A), the Texas Legislative Council; and

(B) for legal material described by Subdivision (2)(B) or (C), the secretary of state.

(4) "Publish" means displaying, presenting, or releasing to the public, or causing to be displayed, presented, or released to the public, legal material by the official publisher.

(5) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Sec. 2051.153. APPLICABILITY. (a) This subchapter applies to all legal material in an electronic record that is:

(1) designated as official by the official publisher under Section 2051.154; and

(2) first published electronically by the official publisher on or after January 1, 2021.

(b) The official publisher is not required to publish legal material on or before the date on which the legal material takes effect.

Sec. 2051.154. LEGAL MATERIAL IN OFFICIAL ELECTRONIC RECORD. (a) If the official publisher publishes legal material only in an electronic record, the official publisher shall:

(1) designate the electronic record as official; and

(2) comply with Sections 2051.155, 2051.157, and 2051.158.

(b) If the official publisher publishes legal material in an electronic record and also publishes the material in a record other than an electronic record, the official publisher may designate the electronic record as official if the official publisher complies with Sections 2051.155, 2051.157, and 2051.158.

Sec. 2051.155. AUTHENTICATION OF OFFICIAL ELECTRONIC RECORD. (a) If the official publisher designates an electronic record as official in accordance with Section 2051.154, the official publisher shall authenticate the record.

(b) The official publisher authenticates an electronic record by providing a method with which a person viewing the electronic record is able to determine that the electronic record is unaltered from the official record published by the official publisher.

Sec. 2051.156. EFFECT OF AUTHENTICATION. (a) Legal material in an electronic record that is authenticated as provided

by Section 2051.155 is presumed to be an accurate copy of the legal material.

(b) If another state has adopted a law that is substantially similar to this subchapter, legal material in an electronic record that is authenticated in that state is presumed to be an accurate copy of the legal material.

(c) A party contesting the authenticity of legal material in an electronic record authenticated as provided by Section 2051.155 has the burden of proving by a preponderance of the evidence that the record is not authentic.

Sec. 2051.157. PRESERVATION AND SECURITY OF LEGAL MATERIAL IN OFFICIAL ELECTRONIC RECORD. (a) The official publisher of legal material in an electronic record designated as official in accordance with Section 2051.154 shall provide for the preservation and security of the record in an electronic form or in a form that is not electronic.

(b) If legal material is preserved under Subsection (a) in an electronic record, the official publisher shall:

(1) ensure the integrity of the record;

(2) provide for backup and disaster recovery of the record; and

(3) ensure the continuing usability of the legal material in the record.

Sec. 2051.158. PUBLIC ACCESS. The official publisher of legal material in an electronic record that is required to be preserved under Section 2051.157 shall ensure that the material is reasonably available for use by the public on a permanent basis.

Sec. 2051.159. STANDARDS. In implementing this subchapter, the official publisher of legal material in an electronic record shall consider:

(1) the standards and practices of other jurisdictions;

(2) the most recent standards regarding authentication, preservation, and security of and public access to legal material in an electronic record and other electronic records, as adopted by national standard-setting bodies;

(3) the needs of users of legal material in electronic records;

(4) the views of governmental officials and entities and other interested persons; and

(5) to the extent practicable, the methods and technologies for the authentication, preservation, and security of and public access to legal material that are compatible with the methods and technologies used by official publishers in other states that have adopted a law that is substantially similar to this subchapter.

Sec. 2051.160. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this subchapter, consideration must be given to the need to promote uniformity of the law with respect to the subject matter of this subchapter among states that enact a law similar to this subchapter.

Sec. 2051.161. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This subchapter modifies, limits, and supersedes the federal Electronic Signatures in Global and National

Commerce Act (15 U.S.C. Section 7001 et seq.) but does not modify, limit, or supersede Section 101(c) of that Act (15 U.S.C. Section 7001(c)) or authorize electronic delivery of any of the notices described in Section 103(b) of that Act (15 U.S.C. Section 7003(b)).

SECTION 11. Section 2054.059, Government Code, is amended to read as follows:

Sec. 2054.059. CYBERSECURITY. From available funds, the department, in consultation with the Information Technology Council for Higher Education, shall:

(1) establish and administer a clearinghouse for information relating to all aspects of protecting the cybersecurity of state agency information;

(2) develop strategies and a framework for:

(A) the securing of cyberinfrastructure by state agencies, including critical infrastructure; and

(B) cybersecurity risk assessment and mitigation planning;

(3) develop and provide training to state agencies, including training for new employees of state agencies, on cybersecurity measures and awareness;

(4) provide assistance to state agencies on request regarding the strategies and framework developed under Subdivision (2); and

(5) promote public awareness of cybersecurity issues.

SECTION 12. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.069 to read as follows:

Sec. 2054.069. SECURITY GUIDANCE FOR INTERNET CONNECTIVITY OF CERTAIN OBJECTS. (a) The department, in consultation with representatives of the information technology industry, voluntary standards organizations, the 10 state agencies that received the most state appropriations for that state fiscal year as determined by the Legislative Budget Board, and the Information Technology Council for Higher Education, shall develop comprehensive risk management guidance 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 guidance 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 13. Section 2054.1184, Government Code, is amended to read as follows:

Sec. 2054.1184. ASSESSMENT OF MAJOR INFORMATION RESOURCES PROJECT. (a) A state agency proposing to spend appropriated funds for a major information resources project must first conduct an evidence-based execution capability assessment using a scoring method delivered by an independent third party to:

(1) determine the agency's capability for implementing the project;

(2) reduce the agency's financial risk in implementing the project; and

(3) increase the probability of the agency's successful implementation of the project.

(b) A state agency shall submit to the department, the quality assurance team established under Section 2054.158, and the Legislative Budget Board a detailed report that includes measurement and corrective actions for [~~identifies~~] the agency's operational and technical [~~organizational~~] strengths and any weaknesses that will be addressed before the agency initially spends appropriated funds for a major information resources project.

(c) Based on project costs, risks, and technical difficulty, the department may require a [~~A~~] state agency to [~~may~~] contract with an independent third party to conduct the assessment under Subsection (a) and prepare the report described by Subsection (b).

(d) The department may allow state agencies to purchase an execution capability assessment using the purchasing method described by Section 2157.068 for commodity items.

SECTION 14. Subchapter F, Chapter 2054, Government Code, is amended by adding Sections 2054.137, 2054.138, and 2054.139 to read as follows:

Sec. 2054.137. INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM. (a) In this section:

(1) "Common control" means a security control that is inherited by one or more information resources technologies.

(2) "Program" means the information security continuous monitoring program described by this section.

(b) Each state agency shall:

(1) develop and maintain an information security

continuous monitoring program that:

(A) allows the agency to maintain ongoing awareness of the security and vulnerabilities of and threats to the agency's information resources;

(B) provides a clear understanding of organizational risk and helps the agency set priorities and manage the risk consistently;

(C) addresses how the agency conducts ongoing authorizations of information resources technologies and the environments in which those technologies operate, including the agency's use of common controls;

(D) aligns with the continuous monitoring guidance, cybersecurity framework, and risk management framework published in Special Publications 800-137 and 800-53 by the United States Department of Commerce National Institute of Standards and Technology;

(E) addresses critical security controls, including hardware asset management, software asset management, configuration management, and vulnerability management; and

(F) requires the integration of cybersecurity products;

(2) establish a strategy and plan to implement a program for the agency;

(3) to the extent practicable, establish information security continuous monitoring as an agency-wide solution and deploy enterprise information security continuous monitoring products and services;

(4) submit specified summary-level security-related information to the dashboard established under Subsection (c)(3);

(5) evaluate and upgrade information resources technologies and deploy new products, including agency and component information security continuous monitoring dashboards, as necessary to support information security continuous monitoring and the need to submit security-related information requested by the department;

(6) require that external service providers hosting state information meet state information security requirements for information security continuous monitoring; and

(7) ensure the agency has adequate staff with the necessary training to meet the objectives of the program.

(c) The department, in consultation with the Information Technology Council for Higher Education, shall:

(1) oversee the implementation of this section by each state agency;

(2) monitor and assist each state agency in implementation of a program and related strategies; and

(3) establish a summary-level statewide dashboard for information security continuous monitoring that provides:

(A) a government-wide view of information security continuous monitoring; and

(B) technical specifications and guidance for state agencies on the requirements for submitting information for purposes of the dashboard.

Sec. 2054.138. CYBERSECURITY THREAT SIMULATION EXERCISES.

(a) In this section, "executive staff" means the management or senior level staff members of a state agency who directly report to the executive head of a state agency.

(b) The executive head of a state agency and members of the executive staff may participate in cybersecurity threat simulation exercises with the agency's information resources technologies employees to test the cybersecurity capabilities of the agency.

Sec. 2054.139. CYBERSECURITY TRAINING FOR NEW EMPLOYEES. Not later than the 30th day after the date on which a new employee begins employment with a state agency, the employee shall complete the cybersecurity training developed by the department under Section 2054.059.

SECTION 15. 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 16. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.5155, 2054.519, 2054.5191, and 2054.5192 to read as follows:

Sec. 2054.5155. 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 to conduct tests to practice securing systems and notifying all affected parties in the event of a data breach; and

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

(b) The department shall include at least one institution of higher education in the list of independent third parties under Subsection (a)(1).

(c) The department annually shall compile the results of the independent risk assessments conducted in the preceding year and prepare:

(1) a public report on the general security issues covered by the assessments that does not contain any information the release of which may compromise any state agency's information resources system; and

(2) a confidential report on specific risks and vulnerabilities that is exempt from disclosure under Chapter 552.

(d) The department annually shall submit to the legislature a comprehensive report on the results of the independent risk assessments conducted under Subsection (a) during the preceding year that includes the report prepared under Subsection (c)(1) and that identifies systematic or pervasive security risk vulnerabilities across state agencies and recommendations for addressing the vulnerabilities but does not contain any information the release of which may compromise any state agency's information resources system.

Sec. 2054.519. 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. 2054.5191. CYBERSTAR PROGRAM; CERTIFICATE OF APPROVAL. (a) The state cybersecurity coordinator, in collaboration with the cybersecurity council and public and private entities in this state, shall develop best practices for cybersecurity that include:

(1) measureable, flexible, and voluntary cybersecurity risk management programs for public and private entities to adopt to prepare for and respond to cyber incidents that

compromise the confidentiality, integrity, and availability of the entities' information systems;

(2) appropriate training and information for employees or other individuals who are most responsible for maintaining security of the entities' information systems;

(3) consistency with:

(A) for a municipality or county, the multihazard emergency operations plan and the safety and security audit required under Section 364.0101, Local Government Code; and

(B) the National Institute of Standards and Technology standards for cybersecurity;

(4) public service announcements to encourage cybersecurity awareness; and

(5) coordination with local and state governmental entities.

(b) The state cybersecurity coordinator shall establish a cyberstar certificate program to recognize public and private entities that implement the best practices for cybersecurity developed in accordance with Subsection (a). The program must allow a public or private entity to submit to the department a form certifying that the entity has complied with the best practices and the department to issue a certificate of approval to the entity. The entity may include the certificate of approval in advertisements and other public communications.

(c) The state cybersecurity coordinator shall conduct an annual public event to promote best practices for cybersecurity.

Sec. 2054.5192. 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 17. Subchapter Q, Chapter 2054, Government Code, is amended by adding Section 2054.577 to read as follows:

Sec. 2054.577. TEXAS INNOVATION FUND AND STATE AGENCY TECHNOLOGY UPGRADES ACCOUNT. (a) In this section:

(1) "Account" means the state agency technology upgrades account.

(2) "Board" means the Texas innovation fund board.

(3) "Cloud computing service" has the meaning assigned by Section 2157.007.

(4) "Device-as-a-service" means a managed service in which hardware that belongs to a managed service provider is installed at a state agency and a service level agreement defines the responsibilities of each party to the agreement.

(5) "Fund" means the Texas innovation fund.

(6) "Information technology system" means any equipment or interconnected system or subsystem of equipment used by a state agency, or a person under a contract with a state agency if the contract requires use of the equipment, to acquire, store, analyze, evaluate, manipulate, manage, move, control, display, switch, interchange, transmit, print, copy, scan, or receive data or other information. The term:

(A) includes a computer, a device-as-a-service

solution, ancillary computer equipment such as imaging, printing, scanning, and copying peripherals and input, output, and storage devices necessary for security and surveillance, peripheral equipment designed to be controlled by the central processing unit of a computer, software and firmware and similar procedures, and services, including support services, and related resources; and

(B) does not include equipment acquired by a contractor incidental to a state contract.

(7) "Legacy information technology system" means an information technology system that is operated with obsolete or inefficient hardware or software technology.

(8) "Qualifying information technology modernization project" means a project by a state agency to:

(A) replace the agency's information technology systems;

(B) transition the agency's legacy information technology systems to a cloud computing service or other innovative commercial platform or technology; or

(C) develop and implement a method to provide adequate, risk-based, and cost-effective information technology responses to threats to the agency's information security.

(9) "State agency" has the meaning assigned by Section 2254.151, notwithstanding Section 2054.003.

(b) The Texas innovation fund board is established to administer the Texas innovation fund and the state agency technology upgrades account and to make awards of financial assistance to state agencies from the fund or account for

qualifying information technology modernization projects. The board is composed of:

(1) one member who is a representative of the department, appointed by the presiding officer of the governing board of the department;

(2) one member who is a representative of the office of the governor, appointed by the governor;

(3) two members of the senate, appointed by the lieutenant governor;

(4) two members of the house of representatives, appointed by the presiding officer of the governing board of the department from a list provided by the speaker of the house of representatives; and

(5) one public member, appointed by the governor.

(c) Members of the board serve staggered six-year terms. A board member is not entitled to compensation for service on the board but is entitled to reimbursement of expenses incurred while performing duties as a board member.

(d) The Texas innovation fund and the state agency technology upgrades account are special funds outside the state treasury to be used by the board, without further legislative appropriation, as provided by this section.

(e) The fund consists of:

(1) money appropriated, credited, or transferred to the fund by the legislature;

(2) money received by the board for the repayment of a loan made from the fund; and

(3) interest and other earnings earned on deposits and investments of money in the fund.

(f) The account consists of:

(1) money deposited to the account by the comptroller in the manner prescribed by Subsection (h); and

(2) interest and other earnings earned on deposits and investments of money in the account.

(g) The department by rule shall establish a loan program to authorize the board to use money from the fund to provide loans to state agencies for qualifying information technology modernization projects. A state agency must apply to the board for a loan from the fund. The application must include a description of the qualifying information technology modernization project for which the state agency is requesting a loan. A loan agreement entered into under this subsection must require the state agency to:

(1) repay the loan to the board within seven years of the date the loan is made to the agency; and

(2) make annual reports to the board identifying cost savings realized by the agency as a result of the project for which the agency received the loan.

(h) At the end of each state fiscal year, on the written request of a state agency, the comptroller shall deposit to the account the unexpended balance of any money appropriated to the agency for that state fiscal year that is budgeted by the agency for information technology services or cybersecurity purposes. A state agency may request money from the account from the board at any time for a qualifying information technology modernization project.

This subsection does not apply to the unexpended balance of any money appropriated to a state agency from federal funds or from a fund created by the constitution of this state.

(i) The comptroller shall separately account for the amount of money deposited to the account at the request of each state agency under Subsection (h). Money deposited to the account under Subsection (h) and any interest and other earnings on that money may be provided only to the state agency for which the comptroller deposited the money to the account and may be used by the agency only for a qualifying information technology modernization project.

(j) Any money deposited to the account at the request of a state agency under Subsection (h) that is not requested by the agency within two years from the date the money is deposited shall be transferred by the comptroller to the general revenue fund to be used in accordance with legislative appropriation.

(k) A state agency that receives money from the fund or the account may collaborate with one or more other state agencies that also receive money from the fund or the account to purchase information technology systems that may be shared between the agencies.

(l) The department and the comptroller may adopt rules to implement and administer this section.

SECTION 18. Chapter 2054, Government Code, is amended by adding Subchapter R to read as follows:

SUBCHAPTER R. INFORMATION RESOURCES OF GOVERNMENTAL ENTITIES

Sec. 2054.601. USE OF NEXT GENERATION TECHNOLOGY. Each

state agency and local government shall, in the administration of the agency or local government, consider using next generation technologies, including cryptocurrency, blockchain technology, and artificial intelligence.

Sec. 2054.602. LIABILITY EXEMPTION. A person who in good faith discloses to a state agency or other governmental entity information regarding a potential security issue with respect to the agency's or entity's information resources technologies is not liable for any civil damages resulting from disclosing the information unless the person stole, retained, or sold any data obtained as a result of the security issue.

Sec. 2054.603. MATCHING GRANTS FOR LOCAL CYBERSECURITY PROJECTS. (a) In this section, "local governmental entity" means a political subdivision of the state, including a:

(1) county;

(2) municipality;

(3) public school district; or

(4) special-purpose district or authority.

(b) Using available funds, the governor shall establish and administer a cybersecurity matching grant program to award grants to local governmental entities to defray the costs of cybersecurity projects.

(c) A local governmental entity that applies to the office of the governor for a matching grant under this section must identify the source and amount of the local governmental entity's matching funds. If the office approves a grant application, the office shall award to the local governmental entity a grant amount

equal to 150 percent of the amount committed by the entity.

(d) The office may set a deadline for grant applications for each state fiscal year.

(e) The governor shall adopt rules to implement the grant program created under this section.

Sec. 2054.604. CYBERSECURITY THREAT ASSESSMENT. The department shall develop a cybersecurity threat assessment for local governments that provides best practices for preventing cybersecurity attacks.

Sec. 2054.605. REPOSITORY FOR CYBERSECURITY EDUCATION AND TRAINING. The department, in conjunction with institutions of higher education as defined by Section 61.003, Education Code, shall maintain and promote a centralized repository of information on cybersecurity education and training that is available to any governmental entity in this state.

SECTION 19. Subchapter B, Chapter 2155, Government Code, is amended by adding Section 2155.092 to read as follows:

Sec. 2155.092. VENDOR STATEMENT 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 statement providing whether, at the time of submitting the bid, offer, proposal, or expression of interest, the vendor has actual knowledge of a confirmed security vulnerability or defect in the device's hardware, software, or firmware that

would adversely affect the security of state data and is subject to an applicable notification law.

(c) If a security vulnerability or defect is identified by a vendor under Subsection (b), the contracting state agency may request additional information in order to assess:

(1) the potential impact of the vulnerability or defect on the agency's planned use of the device; and

(2) whether a security patch or other means of mitigation is currently available or expected within a specific period of time.

SECTION 20. The heading to Section 2157.007, Government Code, is amended to read as follows:

Sec. 2157.007. [~~CONSIDERATION OF~~] CLOUD COMPUTING SERVICE [~~PURCHASE~~].

SECTION 21. Section 2157.007, Government Code, is amended by amending Subsections (a) and (b) and adding Subsections (b-1), (b-2), and (f) to read as follows:

(a) In this section:

(1) "Cloud computing service" has the meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology, as the definition existed on January 1, 2015.

(2) "Major information resources project" has the meaning assigned by Section 2054.003.

(b) Except as provided by Subsection (b-1), a [~~A~~] state agency shall ensure [~~consider cloud computing service options, including any security benefits and cost savings associated with~~

~~purchasing those service options from a cloud computing service provider and from a statewide technology center established by the department~~], when making purchases for an automated information system or a major information resources project, that the system or project is capable of being deployed and run on cloud computing services [~~under Section 2054.118~~].

(b-1) When making a purchase for an automated information system or a major information resources project, a state agency may determine that, due to integration limitations with legacy systems, security risks, costs, or other relevant considerations, the agency is unable to purchase a system or project capable of being deployed and run on cloud computing services.

(b-2) At least 14 days before the date a state agency solicits bids, proposals, offers, or other applicable expressions of interest for a purchase described by Subsection (b-1), the agency shall submit to the Legislative Budget Board for the purchase of an automated information system or to the quality assurance team as defined by Section 2054.003 for the purchase of a major information resources project a report that describes the purchase and the agency's reasoning for making the purchase.

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

must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing or other storage services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 22. 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) Section 364.0053;

(2) Section 364.0102; and

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

SECTION 23. 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. REGIONAL INFORMATION SHARING AND ANALYSIS CENTERS

Sec. 364.0051. ESTABLISHMENT. (a) The cybersecurity coordinator shall provide for the establishment and operation of not more than 20 regional information sharing and analysis centers.

(b) Regional information sharing and analysis centers shall be located throughout the state so that the boundaries for each center are coextensive with the regional education service centers established under Chapter 8, Education Code.

Sec. 364.0052. MEMBERSHIP. Each municipality with a population of more than 25,000 shall join the regional information sharing and analysis center in which the municipality is predominantly located. Any other political subdivision may join the regional information sharing and analysis center in which the political subdivision is predominantly located.

Sec. 364.0053. SECURITY BREACH NOTIFICATION. (a) 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 regional information sharing and analysis center of the breach. The notification must describe the breach, suspected breach, or unauthorized exposure.

(b) A regional information sharing and analysis center 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. 364.0054. 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 office of homeland security. 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 PAYMENT. (a) In this section, "ransomware" has the meaning assigned by Section 33.023, Penal Code.

(b) Not later than 48 hours after the time a political subdivision makes a ransomware payment, the political subdivision shall notify the cybersecurity coordinator of the payment.

SECTION 24. Section 2054.513, Government Code, is repealed.

SECTION 25. The Department of Information Resources shall conduct a study on the types of objects embedded with computing devices that are connected to the Internet that are purchased through the department. The Department of Information Resources shall submit a report on the study to the legislature not later than December 31, 2020.

SECTION 26. (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;

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

(4) information technology procurement.

(b) Not later than November 30, 2019:

(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 12, 2021.

(e) This section expires September 1, 2021.

SECTION 27. As soon as practicable after the effective date of this Act, the governor shall appoint a chief innovation officer as required by Section 401.106, Government Code, as added by this Act.

SECTION 28. (a) An official publisher in the executive branch of state government shall comply with the applicable provisions of Subchapter E, Chapter 2051, Government Code, as added by this Act, in accordance with an implementation plan developed under Subsection (b) of this section.

(b) The Texas State Library and Archives Commission and an official publisher in the executive branch of state government are jointly responsible for developing an implementation plan for the applicable provisions of Subchapter E, Chapter 2051, Government Code, as added by this Act. The implementation plan must:

(1) for each applicable type of legal material defined by Subchapter E, Chapter 2051, Government Code, as added by this Act, advise as to the method by which the legal material may be authenticated, preserved, and made available on a permanent basis; and

(2) establish a timeline for the official publisher to comply with Sections 2051.154, 2051.155, 2051.157, and 2051.158,

Government Code, as added by this Act.

(c) The implementation plan developed under Subsection (b) of this section may provide for compliance by an official publisher in the executive branch of state government with Sections 2051.154, 2051.155, 2051.157, and 2051.158, Government Code, as added by this Act, to be phased in over a period of time.

(d) The Texas State Library and Archives Commission shall provide the implementation plan developed under Subsection (b) of this section to the legislature not later than September 1, 2020.

SECTION 29. (a) An official publisher in the legislative branch of state government shall comply with the applicable provisions of Subchapter E, Chapter 2051, Government Code, as added by this Act, in accordance with an implementation plan developed under Subsection (b) of this section.

(b) An official publisher in the legislative branch of state government, in consultation with the lieutenant governor, the speaker of the house of representatives, the Senate Committee on Administration, and the House Committee on Administration, shall develop an implementation plan for the applicable provisions of Subchapter E, Chapter 2051, Government Code, as added by this Act. The implementation plan must:

(1) for each applicable type of legal material defined by Subchapter E, Chapter 2051, Government Code, as added by this Act, recommend the method by which the legal material may be authenticated, preserved, and made available on a permanent basis; and

(2) establish a timeline for the official publisher to

comply with Sections 2051.154, 2051.155, 2051.157, and 2051.158, Government Code, as added by this Act.

(c) The implementation plan developed under Subsection (b) of this section may provide for compliance by an official publisher in the legislative branch of state government with Sections 2051.154, 2051.155, 2051.157, and 2051.158, Government Code, as added by this Act, to be phased in over a period of time.

(d) An official publisher in the legislative branch of state government shall provide the implementation plan developed under Subsection (b) of this section to the lieutenant governor and speaker of the house of representatives not later than September 1, 2020.

SECTION 30. Section 2054.139, Government Code, as added by this Act, requiring a new employee of a state agency to complete cybersecurity training, applies only to an employee who begins employment on or after the effective date of this Act.

SECTION 31. 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 32. Section 2157.007, Government Code, as amended by this Act, applies only with respect to a purchase made by a state agency on or after the effective date of this Act. A purchase made before the effective date of this Act is governed by the law in effect on the date the purchase was made, and the former law is continued in effect for that purpose.

SECTION 33. If before implementing any provision of this Act a state agency determines that a waiver or authorization from a federal agency is necessary for implementation of that provision, the agency affected by the provision shall request the waiver or authorization and may delay implementing that provision until the waiver or authorization is granted.

SECTION 34. This Act takes effect September 1, 2019.