By: Capriglione 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, 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. 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 8. 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 9. Section 2054.059, Government Code, is amended to read as follows:

Sec. 2054.059. CYBERSECURITY. From available funds, the department 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 10. Subchapter C, Chapter 2054, Government Code, is

amended by adding Section 2054.069 to read as follows:

Sec. 2054.069. SECURITY STANDARDS FOR INTERNET CONNECTIVITY OF CERTAIN OBJECTS. (a) The department, in consultation with representatives of the information technology industry and voluntary standards organizations, shall develop a comprehensive set of risk-based security standards for the Internet connectivity of computing devices embedded in objects used or purchased by state agencies.

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

SECTION 11. 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 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 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 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 fifth business 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 12. 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 13. 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 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.

(c) 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 (b)(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) written acknowledgment of any known cybersecurity risks associated with the technology identified in the test conducted under Section 2054.516 or 2054.517;

(2) proof that any individual servicing the contract holds the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(3) a strategy for mitigating any technology or personnel-related cybersecurity risk identified in the test conducted under Section 2054.516 or 2054.517; and

(4) 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 responsibilities, capacities, and policies 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) minimum training requirements and information for employees or other individuals who are most responsible for maintaining security of the entities' information systems;

(3) compliance 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 14. 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 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 15. 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 16. The heading to Section 2157.007, Government Code, is amended to read as follows:

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

SECTION 17. Section 2157.007, Government Code, is amended by amending Subsection (b) and adding Subsection (f) to read as follows:

(b) 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 under Section 2054.118, that the system or project is capable of being deployed and run on cloud computing services.

(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 under Section 2054.118 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 18. 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 19. 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 20. Section 2054.513, Government Code, is repealed.

SECTION 21. 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 22. (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 23. 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 24. 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 25. 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 26. 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 27. This Act takes effect September 1, 2019.