BILL ANALYSIS

C.S.H.B. 4214
By: Capriglione
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

It has been noted that local government entities and smaller state agencies do not have adequate funding to keep up with cybersecurity, information resources, and emergency planning needs. C.S.H.B. 4214 seeks to provide assistance with those needs by, among other provisions, providing for the appointment of a state chief innovation officer, providing for the creation of information sharing and analysis centers, and establishing a matching grant program for local governments to defray the costs of cybersecurity projects.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Texas Higher Education Coordinating Board in SECTION 2, to the Department of Information Resources in SECTION 13, to the governor in SECTION 14, and to the state cybersecurity coordinator in SECTION 19 of this bill.

ANALYSIS

C.S.H.B. 4214 amends the Education Code to require the safety and security audit conducted by each public school district and public junior college district at least once every three years to include an information technology cybersecurity assessment.

C.S.H.B. 4214 requires the Texas Higher Education Coordinating Board, in consultation with the Department of Information Resources (DIR), to coordinate with public junior colleges, public state colleges, public technical institutes, 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 such institutions of higher education. The bill authorizes the coordinating board to adopt rules as necessary for the administration of this requirement.

C.S.H.B. 4214 amends the Government Code to require the governor to appoint a chief innovation officer. The bill sets out the officer's required duties, which include developing procedures and processes to improve internal state government efficiency and performance and developing methods to improve the experience of residents, businesses, and local governments in interacting with state government.

C.S.H.B. 4214 includes a cyber attack among the events the occurrence or imminent threat of which constitutes a disaster for purposes of the Texas Disaster Act of 1975.

C.S.H.B. 4214 requires the Homeland Security Council, in cooperation with DIR, to conduct a study regarding cyber incidents, as defined by the bill, and significant cyber incidents, as defined by the bill, affecting state agencies and critical infrastructure that is owned, operated, or controlled by agencies and to develop a related comprehensive state response plan. The bill requires the council, not later than September 1, 2020, to deliver the response plan and a report on the findings of the study to applicable public officers. The bill establishes that the response plan and the report are not public information for purposes of state public information law. These provisions expire December 1, 2020.

C.S.H.B. 4214 authorizes the governor to command the Texas National Guard to assist the Texas State Guard with defending the state's cyber operations for purposes of serving the state and safeguarding the public from malicious cyber activity.

C.S.H.B. 4214 authorizes a state agency to 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.

C.S.H.B. 4214 includes training for new state agency employees on cybersecurity measures and awareness among the training DIR is required to develop and provide to state agencies from available funds. The bill requires a new state agency employee, not later than the 30th day after the date the employee's employment begins, to complete the cybersecurity training.

C.S.H.B. 4214 requires DIR, 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 the state fiscal year as determined by the Legislative Budget Board, to 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. The bill requires DIR, in developing the program, to 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.

C.S.H.B. 4214 provides for the required development and maintenance of an information security continuous monitoring program by each state agency. The bill requires DIR to take the following actions:

- oversee the implementation of each agency's monitoring program;
- monitor and assist each agency in implementing the program and related strategies; and
- establish a statewide dashboard for information security continuous monitoring that meets certain requirements.

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

C.S.H.B. 4214 requires the cybersecurity council to ensure all middle and high schools have knowledge of and access to free cybersecurity courses and curriculum approved by the Texas Education Agency, state and regional information sharing and analysis centers, and contracting benefits.

C.S.H.B. 4214 requires each state agency, at least once every five years and in accordance with DIR rules, to take the following actions:

- contract with an independent third party selected from a list provided by DIR to do the following:
    - conduct an independent risk assessment of the agency's exposure to security risks in the agency's information resources systems; and

    - conduct tests to practice securing systems and notifying all affected parties in the event of a data breach; and
- submit the results of the assessment to DIR.

C.S.H.B. 4214 requires DIR to annually compile the results of assessments conducted in the preceding year and to prepare both 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 a confidential report on specific risks and vulnerabilities that is exempt from disclosure under state public information law. The bill requires DIR to annually submit to the legislature a comprehensive report on the results of assessments conducted during the preceding year that includes the public report and that identifies systematic or pervasive security risk vulnerabilities across state agencies and recommendations for addressing the vulnerabilities but that does not contain any information the release of which may compromise any state agency's information resources system.

C.S.H.B. 4214 makes a vendor that contracts with the state to provide information resources technology for a state agency at a cost of $1 million or more responsible for addressing known cybersecurity risks associated with the technology and for any cost associated with addressing identified cybersecurity risks. The bill requires the vendor for a major information resources project to provide to state agency contracting personnel a written attestation regarding the vendor's cybersecurity risk management program and vulnerability management program and an initial summary of certain cybersecurity costs following a risk assessment.

C.S.H.B. 4214 repeals provisions authorizing the state cybersecurity coordinator to establish a voluntary program that recognizes private and public entities functioning with exemplary cybersecurity practices. The bill requires the coordinator, in collaboration with the cybersecurity council and public and private entities in Texas, to develop best practices for cybersecurity and sets out certain requirements for the contents of those best practices. The bill requires the cybersecurity coordinator to conduct an annual public event to promote best practices for cybersecurity and to establish a cyberstar certificate program to recognize entities that implement the best practices. The bill requires the program to allow an entity to submit to DIR a form certifying that the entity has complied with the best practices and to allow DIR to issue the entity a certificate of approval. The bill authorizes the entity to include the certificate in advertisements and other public communications.

C.S.H.B. 4214 requires each state agency that maintains a publicly accessible website that requires submission of sensitive personally identifiable information to use an encrypted secure communication protocol, including a secure hypertext transfer protocol.

C.S.H.B. 4214 requires each state agency and local government to consider using next generation technologies in its administration. The bill exempts a person who in good faith discloses to a governmental entity information regarding a potential security issue with respect to the entity's information resources technologies from civil liability resulting from disclosing the information unless the person stole, retained, or sold any data obtained as a result of the security issue.

C.S.H.B. 4214 requires the governor, using available funds, to establish and administer a cybersecurity matching grant program to award grants to local governmental entities to defray the costs of cybersecurity projects. The bill requires an entity that applies for a grant to identify the source and amount of the entity's matching funds and, if the governor's office approves the application, requires the office of the governor to award to the entity a grant amount equal to 150 percent of the amount committed by the entity. The bill authorizes the office to set a deadline for grant applications for each state fiscal year and requires the governor to adopt rules to implement the grant program.

C.S.H.B. 4214 requires DIR to develop a cybersecurity threat assessment for local governments that provides best practices for preventing cybersecurity attacks. The bill requires DIR, in conjunction with public institutions of higher education, to maintain and promote a centralized repository of information on cybersecurity education and training that is available to any governmental entity in Texas.

C.S.H.B. 4214 requires a vendor offering to sell to the state a good embedded with a computing device capable of Internet connectivity to 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 submission, a hardware, software, or firmware component with any known security vulnerability or defect. This requirement is not applicable to a good provided as part of a major information resources project.

C.S.H.B. 4214 removes the requirement for a state agency to consider cloud computing service options when making purchases for a major information resources project. The bill requires an agency instead to ensure that when making purchases for an automated information system or a major information resources project the system or project is capable of being deployed and run on cloud computing services. The bill requires DIR to 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 agencies to ensure that an agency purchasing a major information resources project selects the most affordable, secure, and efficient storage service available. The bill sets out certain content requirements for the guidelines.

C.S.H.B. 4214 amends the Local Government Code to require the cybersecurity coordinator to provide for the establishment and operation of not more than 20 regional information sharing and analysis centers to be located throughout Texas so that the boundaries for each center are coextensive with the regional education service centers. The bill requires each municipality with a population of more than 25,000 to join the center in which the municipality is predominantly located and authorizes any other political subdivision to join the respective center.

C.S.H.B. 4214 requires a political subdivision, not later than 48 hours after discovering a breach or suspected breach of system security or an unauthorized exposure of sensitive personal information, to notify the center of the breach and requires the notification to describe the breach, suspected breach, or unauthorized exposure. The bill requires a center to report to DIR certain breaches reported by a political subdivision. The bill authorizes the cybersecurity coordinator to adopt rules necessary to implement the bill's provisions regarding the regional information sharing and analysis centers.

C.S.H.B. 4214 requires each municipality or county with a population of more than 100,000 to adopt and implement a multihazard emergency operations plan for use in the municipality's and county's facilities to address mitigation, preparedness, response, and recovery as determined by the cybersecurity council and the governor's office of homeland security. The bill sets out certain requirements for the plan and requires each applicable municipality and county, at least once every three years, to conduct a safety and security audit of the municipality's or county's information technology infrastructure. The bill requires the municipality or county, to the extent possible, to follow safety and security audit procedures developed by the cybersecurity council or a comparable public or private entity and requires a municipality or county to report the results of the audit to the municipality's or county's governing body and to the cybersecurity council. Any document or information collected, developed, or produced during such an audit is not subject to disclosure under state public information law, except that a document relating to a municipality's or county's multihazard emergency operations plan is subject to disclosure under certain specified circumstances.

C.S.H.B. 4214 requires a political subdivision that makes a ransomware payment to notify the cybersecurity coordinator of the payment not later than 48 hours after the payment is made.

C.S.H.B. 4214 requires DIR to conduct a study on the types of objects embedded with computing devices that are connected to the Internet that are purchased through DIR and to submit a report on the study to the legislature not later than December 31, 2020.

C.S.H.B. 4214 requires the lieutenant governor and speaker of the house of representatives to each establish in their respective chambers a Select Committee on Cybersecurity to study, jointly or separately:

- cybersecurity in Texas;
- the information security plans of each state agency;
- the risks and vulnerabilities of state agency cybersecurity; and
- information technology procurement.

The bill provides for the appointment of committee members not later than November 30, 2019, and sets out provisions relating to committee meetings. The bill requires the committees jointly to adopt recommendations on state cybersecurity and report in writing to the legislature any findings and adopted recommendations not later than January 12, 2021. The bill's provisions regarding the select committees expire September 1, 2021.

C.S.H.B. 4214 repeals Section 2054.513, Government Code.

EFFECTIVE DATE

September 1, 2019.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 4214 may differ from the original in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute does not include a requirement for DIR to develop a comprehensive set of risk-based security standards for the Internet connectivity of certain computing devices used or purchased by state agencies, but the substitute includes a requirement for DIR to develop instead a comprehensive risk management program that identifies baseline security features for that Internet connectivity. The substitute includes as a partner with whom DIR must consult in the development of that program the 10 state agencies that received the most state appropriations for that state fiscal year.

The substitute revises the following:

- the date by which a new state agency employee is required to complete the cybersecurity training developed by DIR;
- the information the vendor for a major information resources project is required to provide to state agency contracting personnel; and
- the contents of the cybersecurity best practices developed by the state cybersecurity coordinator.

The substitute specifies that a person's disclosure of information regarding a potential security issue to a state agency or governmental entity for which the person is exempt from liability is made in good faith.