SENATE AMENDMENTS

2nd Printing

By: Capriglione, Elkins, Parker, Dale, Dean, et al. H.B. No. 8

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for state agency information resources.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) state law and applicable rules of any state

agency regarding purchasing guidelines and programs for historically underutilized businesses;

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

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

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

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

(14) an assessment of the agency's cybersecurity practices using information available from the Department of Information Resources or any other appropriate state agency.

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

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

(1) "Cyber incident" means an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information on the computers or systems.

The term includes a vulnerability in implementation or in an information system, system security procedure, or internal control that could be exploited by a threat source.

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

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

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

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

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

(1) the public safety director of the Department of

Public Safety;

(2) the governor;

(3) the lieutenant governor;

(4) the speaker of the house of representatives;

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

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

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

(e) This section expires December 1, 2018.

SECTION 4. Section 551.089, Government Code, is amended to read as follows:

Sec. 551.089. DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING [~~DEPARTMENT OF INFORMATION RESOURCES~~]. This chapter does not require a governmental body [~~the governing board of the Department of Information Resources~~] to conduct an open meeting to deliberate:

(1) security assessments or deployments relating to information resources technology;

(2) network security information as described by Section 2059.055(b); or

(3) the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

SECTION 5. Section 552.139, Government Code, is amended by adding Subsection (d) to read as follows:

(d) When posting a contract on an Internet website as required by Section 2261.253, a state agency shall redact information made confidential by this section or excepted from public disclosure by this section. Redaction under this subsection does not except information from the requirements of Section 552.021.

SECTION 6. 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 7. 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 8. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0594 to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) The department shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) The department shall appoint persons from appropriate

state agencies to serve as representatives to the information sharing and analysis center.

(c) The department, using existing resources, shall provide administrative support to the information sharing and analysis center.

SECTION 9. Section 2054.076, Government Code, is amended by adding Subsection (b-1) to read as follows:

(b-1) The department shall provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training and the industry-recognized certifications that must be completed by all information resources employees of the agencies. The department shall consult with the Information Technology Council for Higher Education on applying the guidelines to institutions of higher education.

SECTION 10. Sections 2054.077(b) and (e), Government Code, are amended to read as follows:

(b) The information resources manager of a state agency shall [~~may~~] prepare or have prepared a report, including an executive summary of the findings of the report, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(e) Separate from the executive summary described by Subsection (b), a state agency [~~whose information resources manager has prepared or has had prepared a vulnerability report~~] shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

SECTION 11. Section 2054.1125(b), Government Code, is amended to read as follows:

(b) A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply[~~, in the event of a breach of system security,~~] with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

(A) the department, including the chief information security officer and the state cybersecurity coordinator; or

(B) if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

SECTION 12. Section 2054.133, Government Code, is amended by adding Subsections (b-1), (b-2), (b-3), and (b-4) to read as follows:

(b-1) The executive head and chief information security officer of each state agency shall annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. The plan at a minimum must include solutions that isolate and segment sensitive information and maintain architecturally sound and secured separation among networks. If a state agency does not have a chief information security officer, the highest ranking information security employee for the agency shall review and approve the plan and strategies. The executive head retains full responsibility for the agency's information security and any risks to that security.

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

(b-3) Each state agency shall include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for

Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. The agency shall, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The agency may incorporate the core functions over a period of years.

(b-4) A state agency's information security plan must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to contractually warrant that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 13. Section 2054.512, Government Code, is amended to read as follows:

Sec. 2054.512. CYBERSECURITY [~~PRIVATE INDUSTRY-GOVERNMENT~~] COUNCIL. (a) The state cybersecurity coordinator shall [~~may~~] establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) The cybersecurity council must include:

(1) one member appointed by the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives; and

(4) additional members appointed by the state cybersecurity coordinator, including representatives of institutions of higher education and private sector leaders.

(c) In appointing representatives from institutions of higher education to the cybersecurity council, the state cybersecurity coordinator shall consider appointing members of the Information Technology Council for Higher Education.

(d) The cybersecurity council shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 14. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.515, 2054.516, 2054.517, 2054.518, and 2054.519 to read as follows:

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

(1) contract with an independent third party selected from a list provided by the department to conduct an independent risk assessment of the agency's exposure to security risks in the agency's information resources systems and 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. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency, other than an institution of higher education subject to Section 2054.517, implementing an Internet website or mobile application that processes any personally identifiable or confidential information must:

(1) submit a data security plan to the department during development and as early as feasible in the testing of the website or application and submit any modification to the plan made during development; and

(2) before deploying the website or application:

(A) subject the website or application to a

vulnerability and penetration test conducted by an independent third party; and

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

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

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

(2) data storage locations;

(3) data interaction with online or mobile devices;

(4) security of data transfer;

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

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

(7) appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing 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.

(c) Unless a state agency has previously submitted a comprehensive security plan approved by the department and has sufficient personnel and technology to review plans internally, the department shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan

to the state agency as soon as practicable after the department reviews the plan.

(d) A data security plan submitted under Subsection (a) and any recommendation for changes made under Subsection (c) are not public information for purposes of Chapter 552.

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Each institution of higher education, as defined by Section 61.003, Education Code, shall adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Before deploying an Internet website or mobile application that processes confidential information for an institution of higher education, the developer of the website or application for the institution must submit to the institution's information security officer the information required under policies adopted by the institution to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the institution's policies must require the developer to submit information describing:

(1) the architecture of the website or application;

(2) the authentication mechanism for the website or application; and

(3) the administrator level access to data included in the website or application.

(c) Before deploying an Internet website or mobile

application described by Subsection (b), an institution of higher education must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Each institution of higher education shall submit to the department the policies adopted as required by Subsection (b). The department shall review the policies and make recommendations for appropriate changes.

Sec. 2054.518. 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 vulnerability and penetration test conducted under Section 2054.516 or Section 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 vulnerability and penetration test conducted under Section 2054.516 or Section 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. 2054.519. CYBERSECURITY RISKS AND INCIDENTS. (a) The department shall develop a plan to address cybersecurity risks and incidents in this state. The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in implementing the components of the plan for which the department lacks resources to address internally. The agreement may include provisions for:

(1) providing fee reimbursement for appropriate industry-recognized certification examinations for and training to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents;

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

(3) delivering to state agency personnel with access to state agency networks routine training related to appropriately protecting and maintaining information technology systems and devices, implementing cybersecurity best practices, and mitigating cybersecurity risks and vulnerabilities;

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

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

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

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

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

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

(d) The department shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 15. Section 2054.575(a), Government Code, is amended to read as follows:

(a) A state agency shall, with available funds, identify

information security issues and develop a plan to prioritize the remediation and mitigation of those issues. The agency shall include in the plan:

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

(2) the best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

(3) analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(4) the level of preparedness of state agency cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

(5) a strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications.

SECTION 16. Section 2059.055(b), Government Code, is amended to read as follows:

(b) Network security information is confidential under this section if the information is:

(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity [~~state agency~~];

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

SECTION 17. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2061 to read as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITIONS. In this chapter:

(1) "Cybersecurity risk" means a material threat of attack, damage, or unauthorized access to the networks, computers, software, or data storage of a state agency.

(2) "State agency" means a department, commission, board, office, council, authority, or other agency in the executive, legislative, or judicial branch of state government, including a university system or institution of higher education, as defined by Section 61.003, Education Code, that is created by the constitution or a statute of this state.

Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) A state agency shall destroy or arrange for the destruction of information that presents a cybersecurity risk and alone or in conjunction with other information identifies an individual in connection with the agency's networks, computers, software, or data storage if the

agency is otherwise prohibited by law from retaining the information for a period of years.

(b) A state agency shall destroy or arrange for the destruction of information described by Subsection (a) in accordance with standards for destruction of data prescribed in the National Security Program Operating Manual, 1995 edition.

(c) This section does not apply to a record involving criminal activity or a criminal investigation retained for law enforcement purposes.

(d) A state agency may not destroy or arrange for the destruction of any election data before the third anniversary of the date the election to which the data pertains is held.

(e) A state agency may not under any circumstance sell:

(1) a person's precise geographic location information;

(2) a person's Internet browsing history;

(3) a person's application usage history; or

(4) the functional equivalent of the information described in Subdivisions (1)-(3).

(f) Not later than September 1, 2019, each state agency shall develop the systems and policies necessary to comply with this section. This subsection expires September 1, 2020.

SECTION 18. Section 2157.007, Government Code, is amended by adding Subsection (e) to read as follows:

(e) The department shall periodically review guidelines on state agency information that may be stored by a cloud computing 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 19. Chapter 276, Election Code, is amended by adding Section 276.011 to read as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552, Government Code; and

(4) submit a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election to the standing

committees of the legislature with jurisdiction over election procedures.

(b) The study must include:

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

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

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

(c) The secretary of state, using existing resources, may contract with a qualified vendor to conduct the study required by this section.

(d) This section expires January 1, 2019.

SECTION 20. (a) The lieutenant governor shall establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives shall establish a House Select Committee on Cybersecurity to, jointly or separately, study:

(1) cybersecurity in this state;

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

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

(b) Not later than November 30, 2017:

(1) the lieutenant governor shall appoint five senators to the Senate Select Committee on Cybersecurity, one of

whom shall be designated as chair; and

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

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

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

(e) This section expires September 1, 2019.

SECTION 21. (a) In this section, "state agency" means a board, commission, office, department, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state. The term does not include a university system or institution of higher education as those terms are defined by Section 61.003, Education Code.

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

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

(1) the current digital data storage practices of

state agencies in this state;

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

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

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

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

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

(7) the security level and possible benefits of and the cost savings from using cloud computing services for agency data storage, data classification, and records management.

(d) Each state agency shall participate in the study required by this section and provide appropriate assistance and information to the Department of Information Resources and the Texas State Library and Archives Commission.

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

representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) This section expires September 1, 2019.

SECTION 22. The changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 23. This Act takes effect September 1, 2017.

ADOPTED

MAY 24 2017

Secretary of the Senate

By: Nelson H.B. No. 8

Substitute the following for __.B. No. _____:

By: Brandon Creighton C.S.__.B. No. _____

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for state agency information resources.

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

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

SECTION 2. Section 551.089, Government Code, is amended to read as follows:

Sec. 551.089. DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING [~~DEPARTMENT OF INFORMATION RESOURCES~~]. This chapter does not require a governmental body [~~the governing board of the Department of Information Resources~~] to conduct an open meeting to deliberate:

(1) security assessments or deployments relating to information resources technology;

(2) network security information as described by Section 2059.055(b); or

(3) the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

SECTION 3. Section 552.139, Government Code, is amended by adding Subsection (d) to read as follows:

(d) When posting a contract on an Internet website as required by Section 2261.253, a state agency shall redact information made confidential by this section or excepted from

public disclosure by this section. Redaction under this subsection does not except information from the requirements of Section 552.021.

SECTION 4. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0594 to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) The department shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) The department shall appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) The department, using funds other than funds appropriated to the department in a general appropriations act, shall provide administrative support to the information sharing and analysis center.

SECTION 5. Sections 2054.077(b) and (e), Government Code, are amended to read as follows:

(b) The information resources manager of a state agency may prepare or have prepared a report, including an executive summary of the findings of the report, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to

which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(e) Separate from the executive summary described by Subsection (b), a state agency [~~whose information resources manager has prepared or has had prepared a vulnerability report~~] shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

SECTION 6. Section 2054.1125(b), Government Code, is amended to read as follows:

(b) A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply[~~, in the event of a breach of system security,~~] with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

(A) the department, including the chief information security officer and the state cybersecurity coordinator; or

(B) if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

SECTION 7. Section 2054.133, Government Code, is amended by adding Subsections (b-1), (b-2), and (b-3) to read as follows:

(b-1) The executive head and information security officer of each state agency shall annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. The plan at a minimum must include solutions that isolate and segment sensitive information and maintain architecturally sound and secured separation among networks. If a state agency does not have an information security officer, the highest ranking information security employee for the agency shall review and approve the plan and strategies. The executive head retains full responsibility for the agency's information security and any risks to that security.

(b-2) Each state agency shall include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. The agency shall, at a minimum, identify any

information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The agency may incorporate the core functions over a period of years.

(b-3) A state agency's information security plan must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to contractually warrant that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules as specified in the applicable scope of work, request for proposal, or other document requirements.

SECTION 8. Section 2054.512, Government Code, is amended to read as follows:

Sec. 2054.512. CYBERSECURITY [~~PRIVATE INDUSTRY-GOVERNMENT~~] COUNCIL. (a) The state cybersecurity coordinator shall [~~may~~] establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) The cybersecurity council must include:

(1) one member who is an employee of the office of the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives; and

(4) additional members appointed by the state cybersecurity coordinator, including representatives of institutions of higher education and private sector leaders.

(c) In appointing representatives from institutions of higher education to the cybersecurity council, the state cybersecurity coordinator shall consider appointing members of the Information Technology Council for Higher Education.

(d) The cybersecurity council shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

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

Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) At least once every two years, each state agency shall conduct an information security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities.

(b) Not later than December 1 of the year in which a state agency conducts the assessment under Subsection (a), the agency shall report the results of the assessment to the department, the governor, the lieutenant governor, and the speaker of the house of representatives.

(c) The department by rule may establish the requirements for the information security assessment and report required by this section.

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

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

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

(2) the best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

(3) an analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(4) the level of preparedness of state agency cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

(5) a strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications.

SECTION 11. Section 2059.055(b), Government Code, is

amended to read as follows:

(b) Network security information is confidential under this section if the information is:

(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity [~~state agency~~];

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

SECTION 12. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2061 to read as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITIONS. In this chapter:

(1) "Cybersecurity risk" means a material threat of attack, damage, or unauthorized access to the networks, computers, software, or data storage of a state agency.

(2) "State agency" means a department, commission, board, office, council, authority, or other agency in the executive, legislative, or judicial branch of state government, including a university system or institution of higher education, as defined by Section 61.003, Education Code, that is created by the constitution or a statute of this state.

Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) A state agency shall destroy or arrange for the destruction of information that

presents a cybersecurity risk and alone or in conjunction with other information identifies an individual in connection with the agency's networks, computers, software, or data storage if the agency is otherwise prohibited by law from retaining the information for a period of years.

(b) This section does not apply to a record involving criminal activity or a criminal investigation retained for law enforcement purposes.

(c) A state agency may not destroy or arrange for the destruction of any election data before the third anniversary of the date the election to which the data pertains is held.

(d) A state agency may not under any circumstance sell:

(1) a person's Internet browsing history;

(2) a person's application usage history; or

(3) the functional equivalent of the information described in Subdivisions (1) and (2).

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

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter

552, Government Code; and

(4) submit to the standing committees of the legislature with jurisdiction over election procedures a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election.

(b) The study must include:

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

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

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

(c) The secretary of state, using existing resources, may contract with a qualified vendor to conduct the study required by this section.

(d) This section expires January 1, 2019.

SECTION 14. (a) The lieutenant governor shall establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives shall establish a House Select Committee on Cybersecurity to, jointly or separately, study:

(1) cybersecurity in this state;

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

(3) the risks and vulnerabilities of state agency

cybersecurity.

(b) Not later than November 30, 2017:

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

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

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

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

(e) This section expires September 1, 2019.

SECTION 15. (a) In this section, "state agency" means a board, commission, office, department, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state. The term does not include a university system or institution of higher education as those terms are defined by Section 61.003, Education Code.

(b) The Department of Information Resources, in consultation with the Texas State Library and Archives Commission,

shall conduct a study on state agency digital data storage and records management practices and the associated costs to this state.

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

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

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

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

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

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

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

(7) the security level and possible benefits of and the cost savings from using cloud computing services for agency data storage, data classification, and records management.

(d) Each state agency shall participate in the study required by this section and provide appropriate assistance and information to the Department of Information Resources and the Texas State Library and Archives Commission.

(e) Not later than December 1, 2018, the Department of

Information Resources shall issue a report on the study required under this section and recommendations for reducing state costs and for improving efficiency in digital data storage and records management to the lieutenant governor, the speaker of the house of representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) This section expires September 1, 2019.

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

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

ADOPTED
MAY 24 2017
Secretary of the Senate

FLOOR AMENDMENT NO. 1 BY: Jane Nelson

Amend C.S.H.B. No. 8 (senate committee printing) by striking all below the enacting clause and substituting the following:

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

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

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

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

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

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

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

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

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

(5) whether less restrictive or alternative methods

of performing any function that the agency performs could adequately protect or provide service to the public;

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

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

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

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

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

(B) state law and applicable rules of any state agency regarding purchasing guidelines and programs for historically underutilized businesses;

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

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

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

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

(14) an assessment of the agency's cybersecurity practices using confidential information available from the Department of Information Resources or any other appropriate state agency.

SECTION 3. Section 551.089, Government Code, is amended to read as follows:

Sec. 551.089. DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING [~~DEPARTMENT OF INFORMATION RESOURCES~~]. This chapter does not require a governmental body [~~the governing board of the Department of Information Resources~~] to conduct an open meeting to deliberate:

(1) security assessments or deployments relating to information resources technology;

(2) network security information as described by Section 2059.055(b); or

(3) the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

SECTION 4. Section 552.139, Government Code, is amended by adding Subsection (d) to read as follows:

(d) When posting a contract on an Internet website as required by Section 2261.253, a state agency shall redact information made confidential by this section or excepted from public disclosure by this section. Redaction under this subsection does not except information from the requirements of Section 552.021.

SECTION 5. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0594 to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) The department shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) The department shall appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) The department, using funds other than funds appropriated to the department in a general appropriations act, shall provide administrative support to the information sharing and analysis center.

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

(b-1) The department shall provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training that must be completed by all information resources employees of the agencies. The department shall consult with the Information Technology Council for Higher Education on applying the guidelines to institutions of higher education.

SECTION 7. Sections 2054.077(b) and (e), Government Code, are amended to read as follows:

(b) The information resources manager of a state agency shall [~~may~~] prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a

computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(e) Separate from the executive summary described by Subsection (b), a state agency [~~whose information resources manager has prepared or has had prepared a vulnerability report~~] shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

SECTION 8. Section 2054.1125(b), Government Code, is amended to read as follows:

(b) A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply[~~, in the event of a breach of system security,~~] with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

(A) the department, including the chief information security officer and the state cybersecurity coordinator; or

(B) if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

SECTION 9. Section 2054.512, Government Code, is amended to read as follows:

Sec. 2054.512. CYBERSECURITY [~~PRIVATE-INDUSTRY-GOVERNMENT~~] COUNCIL. (a) The state cybersecurity coordinator shall [~~may~~] establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) The cybersecurity council must include:

(1) one member who is an employee of the office of the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives; and

(4) additional members appointed by the state cybersecurity coordinator, including representatives of institutions of higher education and private sector leaders.

(c) In appointing representatives from institutions of higher education to the cybersecurity council, the state cybersecurity coordinator shall consider appointing members of the Information Technology Council for Higher Education.

(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.

(e) The cybersecurity council shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 10. Section 2054.133, Government Code, is amended by adding Subsection (e) to read as follows:

(e) Each state agency shall include in the agency's information security plan a written acknowledgment that the executive director or other head of the agency, the chief financial officer, and each executive manager as designated by the state agency have been made aware of the risks revealed during the preparation of the agency's information security plan.

SECTION 11. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.515, 2054.516, 2054.517, and 2054.518 to read as follows:

Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) At least once every two years, each state agency shall conduct an information security assessment of the agency's information resources systems, network systems, digital data

storage systems, digital data security measures, and information resources vulnerabilities.

(b) Not later than December 1 of the year in which a state agency conducts the assessment under Subsection (a), the agency shall report the results of the assessment to the department, the governor, the lieutenant governor, and the speaker of the house of representatives.

(c) The department by rule may establish the requirements for the information security assessment and report required by this section.

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. Each state agency, other than an institution of higher education subject to Section 2054.517, implementing an Internet website or mobile application that processes any sensitive personal information or confidential information must:

(1) submit a biennial data security plan to the department not later than October 15 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Each institution of higher education, as defined by Section 61.003, Education Code, shall adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Before deploying an Internet website or mobile application that processes confidential information for an institution of higher education, the developer of the website or

application for the institution must submit to the institution's information security officer the information required under policies adopted by the institution to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the institution's policies must require the developer to submit information describing:

(1) the architecture of the website or application;

(2) the authentication mechanism for the website or application; and

(3) the administrator level access to data included in the website or application.

(c) Before deploying an Internet website or mobile application described by Subsection (b), an institution of higher education must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Each institution of higher education shall submit to the department the policies adopted as required by Subsection (b). The department shall review the policies and make recommendations for appropriate changes.

Sec. 2054.518. CYBERSECURITY RISKS AND INCIDENTS. (a) The department shall develop a plan to address cybersecurity risks and incidents in this state. The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in implementing the components of the plan for which the department lacks resources to address internally. The agreement may include provisions for:

(1) providing fee reimbursement for appropriate industry-recognized certification examinations for and training

to state agencies preparing for and responding to cybersecurity risks and incidents;

(2) developing and maintaining a cybersecurity risks and incidents curriculum using existing programs and models for training state agencies;

(3) delivering to state agency personnel with access to state agency networks routine training related to appropriately protecting and maintaining information technology systems and devices, implementing cybersecurity best practices, and mitigating cybersecurity risks and vulnerabilities;

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

(5) conducting cybersecurity training and simulation exercises for state agencies to encourage coordination in defending against and responding to cybersecurity risks and incidents;

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

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

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

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

agencies and political subdivisions.

(d) The department shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 12. Section 2054.575(a), Government Code, is amended to read as follows:

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

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

(2) the best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

(3) analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(4) the level of preparedness of state agency cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

(5) a strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications.

SECTION 13. Section 2059.055(b), Government Code, is amended to read as follows:

(b) Network security information is confidential under this section if the information is:

(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity [~~state agency~~];

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

SECTION 14. Chapter 276, Election Code, is amended by adding Section 276.011 to read as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552, Government Code; and

(4) submit to the standing committees of the legislature with jurisdiction over election procedures a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election.

(b) The study must include:

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

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

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

(c) The secretary of state, using existing resources, may contract with a qualified vendor to conduct the study required by this section.

(d) This section expires January 1, 2019.

SECTION 15. (a) The lieutenant governor shall establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives shall establish a House Select Committee on Cybersecurity to, jointly or separately, study:

(1) cybersecurity in this state;

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

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

(b) Not later than November 30, 2017:

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

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

(c) The committees established under this section shall

convene separately at the call of the chair of the respective committees, or jointly at the call of both chairs. In joint meetings, the chairs of each committee shall act as joint chairs.

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

(e) This section expires September 1, 2019.

SECTION 16. (a) In this section, "state agency" means a board, commission, office, department, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state. The term does not include a university system or institution of higher education as those terms are defined by Section 61.003, Education Code.

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

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

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

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

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

policies;

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

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

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

(7) the security level and possible benefits of and the cost savings from using cloud computing services for agency data storage, data classification, and records management.

(d) Each state agency shall participate in the study required by this section and provide appropriate assistance and information to the Department of Information Resources and the Texas State Library and Archives Commission.

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

(f) This section expires September 1, 2019.

SECTION 17. The changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 18. This Act takes effect September 1, 2017.

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 25, 2017

TO: Honorable Joe Straus, Speaker of the House, House of Representatives

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB8** by Capriglione (Relating to cybersecurity for state agency information resources.), **As Passed 2nd House**

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to conduct a risk assessment every two years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost $229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. This analysis assumes the Department of Information Resources (DIR) would have an estimated cumulative cost of $2.2 million and 2.0 additional FTEs for the 2018-19 biennium as a result of requirements to develop plans to address cybersecurity risks and incidents. According to DIR, costs would be funded through the Clearing Fund (Appropriated Receipts), which is generated through administrative fees charged to purchases made through DIR's Cooperative Contracts program. Entities that make purchases through the Cooperative Contracts program include state agencies, institutions of higher education, and local jurisdictions. This analysis assumes that if appropriations do not cover the cost of implementation, DIR would increase administrative fee rates to generate sufficient revenues.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272.0 FTEs perform IT-related projects and training these staff is estimated to cost $791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to conduct a security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities at least once every two years. Each state agency would be required to report the results of the assessment to DIR, the Governor, the Lieutenant Governor, and the Speaker of the House of Representatives by December 1 in the year in which the agency conducts the assessment. The bill would require DIR to establish the requirements for the information security assessment and report.

The bill would also require that each agency conduct a vulnerability and penetration test of each state agency's website or mobile application that processes any personally identifiable or confidential information. This provision could have a cost for some agencies, although the amount would depend on the manner in which it is implemented by the agency.

The bill would require DIR to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DIR's efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. DIR indicated that the agency would need 2.0 additional FTEs to accomplish the provisions of the bill, estimated at $2.2 million for the 2018-19 biennium.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to the Texas Association of Counties, this bill would have no fiscal impact to units of local government.

Source Agencies: 116 Sunset Advisory Commission, 304 Comptroller of Public Accounts, 300 Trusteed Programs Within the Office of the Governor, 313 Department of Information Resources, 320 Texas Workforce Commission, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices

LBB Staff: UP, CL, MMe, BRi

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 19, 2017

TO: Honorable Kelly Hancock, Chair, Senate Committee on Business & Commerce

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB8** by Capriglione (Relating to cybersecurity for state agency information resources.), **Committee Report 2nd House, Substituted**

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to perform an information security risk assessment every two years.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported that the provisions of the bill could be implemented within existing resources.

The bill would require each state agency to conduct a security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities at least once every two years. Each state agency would be required to report the results of the assessment to DIR, the Governor, the Lieutenant Governor, and the Speaker of the House of Representatives by December 1 in the year in which the agency conducts the assessment. The bill would require DIR to establish the requirements for the information security assessment and report.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources and the Texas Medical Board estimated this would cost $50,000 in fiscal year 2019.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to the Texas Association of Counties, this bill would have no fiscal impact to units of local government.

Source Agencies: 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 307 Secretary of State, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: UP, CL, MMe, BRi, RC, JGA

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 10, 2017

TO: Honorable Kelly Hancock, Chair, Senate Committee on Business & Commerce

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB8** by Capriglione (Relating to cybersecurity for state agency information resources.), **As Engrossed**

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of $6.0 million in General Revenue Funds, $1.4 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost $229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. This analysis assumes the Department of Information Resources (DIR) would have an estimated cumulative cost of $5.2 million and 2.0 additional FTEs for the 2018-19 biennium as a result of requirements to develop plans to address cybersecurity risks and incidents. Additionally, if agencies were to utilize DIR's existing third party independent risk assessment services and website and application vulnerability and penetration testing services, the agency estimates an additional cost of $4.0 million for the biennium to expand current offerings of these services. All costs would be funded through the Clearing Fund (Appropriated Receipts), which is generated through administrative fees charged to purchases made through DIR's Cooperative Contracts program. Entities that make purchases through the Cooperative Contracts program include state agencies, institutions of higher education, and local jurisdictions. This analysis assumes DIR would increase administrative fee rates to generate sufficient revenues to cover the costs of implementation.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification.

The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272.0 FTEs perform IT-related projects and training these staff is estimated to cost $791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of $50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of $150,000 to $350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that an independent third party conduct a vulnerability and penetration test of each state agency's (other than an institution higher education) website or mobile application that processes any personally identifiable or confidential information. The Comptroller of Public Accounts estimated third party contracting costs would be $750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of $4.0 million to agencies in the biennium, were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements. This assumes that 187 independent risk assessments would be performed over a five year period at a cost of $48,000 per assessment, and that 20 mobile and application vulnerability tests would be performed per year, at a cost of $10,000 per test.

The bill would require DIR to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DIR's efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. DIR indicated that the agency would need 2.0 additional FTEs to accomplish the provisions of the bill, estimated at $5.2 million for the 2018-19 biennium.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost $50,000 in fiscal year 2019 and DPS reported that 3.0 additional FTEs at a cost of $697,925 would be required for the 2018-19 biennium.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill

would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to DIR, estimated costs of certification examinations for and training to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents could be $3.2 million for the biennium, assuming 1,081 school districts, 900 cities and 256 counties at $2,000 per year. One employee training and certification exam would be conducted per year for one-third of these entities. DIR assumes the cost for the certification examinations and training would be paid out of DIR's Clearing Fund (Appropriated Receipts).

Source Agencies: 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 307 Secretary of State, 313 Department of Information Resources, 320 Texas Workforce Commission, 503 Texas Medical Board, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 781 Higher Education Coordinating Board, 323 Teacher Retirement System, 405 Department of Public Safety, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 701 Texas Education Agency, 720 The University of Texas System Administration

LBB Staff: UP, CL, MMe, PM, LBO, JAW, RC, LCO, GGo, GO

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 14, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB8** by Capriglione (Relating to cybersecurity for state agency information resources.), **Committee Report 1st House, Substituted**

The statewide fiscal implications of the bill cannot be determined at this time, but is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of $6.0 million in General Revenue Funds, $1.4 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost $229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. Requirements that would apply to the Department of Public Safety (DPS) and Department of Information Resources (DIR) are noted below. Based on LBB staff analysis, the cumulative impact to DPS would be a cost of $6.1 million in General Revenue Funds, including an additional 3.0 FTEs, and certain requirements would have significant yet indeterminate costs. No significant fiscal impact is assumed for DIR to accomplish the bill's requirements of them specifically.

The bill would require DPS to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DPS' efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. Based on LBB staff analysis, DPS would require 3.0 additional FTEs to accomplish these provisions at a cost of approximately $0.7 million in General Revenue Funds for the 2018-19 biennium., This analysis assumes DPS would provide fee reimbursement for appropriate industry-recognized certification examinations under the

agreement. According to DPS staff, this would cost an additional $5.2 million in General Revenue Funds, assuming $20 per certification for 260,000 responders.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272 FTEs perform IT-related projects and training these staff is estimated to cost $791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of $50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of $150,000 to $350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that each state agency (other than an institution higher education) website or mobile application processing any personally identifiable or confidential information undergo a vulnerability and penetration test conducted by an independent third party. The Comptroller of Public Accounts estimated third party contracting costs would be $750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of $4.0 million in the biennium were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements, and assumes this would include 20 new vulnerability tests per year at a cost of $10,000 per test.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost $50,000 in fiscal year 2019 and DPS stated the costs related to Intelligence and Counterterrorism Division and Homeland Security responsibilities would be significant but cannot be determined.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the billwould not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 306 Library & Archives Commission, 307 Secretary of State, 710 Texas A&M University System Administrative and General Offices, 781 Higher Education Coordinating Board, 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 720 The University of Texas System Administration

LBB Staff: UP, LBO, MMe, PM, JAW, RC, LCO, GGo, GO

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

March 20, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB8** by Capriglione (Relating to cybersecurity for state agency information resources.), **As Introduced**

The statewide fiscal implications of the bill cannot be determined at this time, but is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. The costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of $22.6 million in General Revenue Funds, $1.3 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost $229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE. Requirements that would apply to the Department of Public Safety (DPS) and Department of Information Resources (DIR) are noted below. Based on LBB staff analysis, the cumulative impact to DPS would be an additional 4.0 FTEs at a cost of $1.0 million in General Revenue Funds, and certain requirements would have significant yet indeterminate costs. No significant fiscal impact is assumed for DIR to accomplish the bill's requirements of them specifically.

The bill would authorize DPS to enter into an agreement with a national organization to address cybersecurity risks and incidents in the state, and authorizes an agreement with an organization to include certain provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. Based on LBB staff analysis, DPS would require 3.0 additional FTEs to accomplish these provisions at a cost of approximately $0.7 million in General Revenue Funds for the 2018-19 biennium.

The bill would require the Homeland Security Council conduct a one-time study regarding cyber

attacks on state agencies and critical infrastructure, and develop a plan agencies would implement in the event of a cyber attack. Based on LBB staff analysis, DPS would incur a one-time cost of approximately $86,647 for 1.0 additional FTE, plus benefits, to assist the Council in completing this requirement.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272 FTEs perform IT-related projects and training these staff is estimated to cost $791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require the executive head and chief information security officer (CISO) of each state agency to annually review the agency's information security plan, develop strategies for information resources systems that are at highest risk for security breaches, and submit these to the Legislative Budget Board. There is no statutory requirement for agencies to have a CISO; therefore some agencies may need additional staff to fulfill this requirement, although the number of additional staff that would be hired is unknown. The average annual salary, without benefits, for a CISO is $119,847 per year.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of $50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of $150,000 to $350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that each state agency website or mobile application processing any personally identifiable or confidential information undergo a vulnerability and penetration test conducted by an independent third party. UT Austin indicated they currently perform 20 to 25 of these types of tests each month in-house. At an estimated $10,000 per external test, they estimate a cost of $2.4 million annually to expand this testing to meet the third party contract requirements of the bill. The Comptroller of Public Accounts estimated third party contracting costs would be $750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of $4.0 million in the biennium were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements, and assumes this would include 20 new vulnerability tests per year at a cost of $10,000 per test.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information identifies an individual, if retention of the information is not required under other law. The cost of this would vary based on how much

personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost $50,000 in fiscal year 2019, and DPS stated the cost would be significant but cannot be determined.

The bill would require the Texas Rangers conduct a one-time study regarding cyber attacks on election infrastructure. DPS staff stated the cost for this would be significant but cannot be determined.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: UP, LBO, MMe, PM, LCO, GGo, GO, RC