By: Capriglione, et al. (Senate Sponsor - Nelson) H.B. No. 8

(In the Senate - Received from the House April 26, 2017; May 3, 2017, read first time and referred to Committee on Business & Commerce; May 19, 2017, reported adversely, with favorable Committee Substitute by the following vote: Yeas 9, Nays 0; May 19, 2017, sent to printer.)

COMMITTEE VOTE

	Yea	Nay	Absent	PNV
Hancock	X			
Creighton	X			
Campbell	X			
Estes	X			
Nichols	X			
Schwertner	X			
Taylor of Galveston	X			
Whitmire	X			
Zaffirini	X			

COMMITTEE SUBSTITUTE FOR H.B. No. 8 By: Creighton

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.

* * * * *