By: Paxton S.B. No. 1779

(In the Senate - Filed March 6, 2019; March 18, 2019, read first time and referred to Committee on Business & Commerce; April 24, 2019, reported favorably by the following vote: Yeas 9, Nays 0; April 24, 2019, sent to printer.)

COMMITTEE VOTE

	Yea	Nay	Absent	PNV
Hancock	X			
Nichols	X			
Campbell	X			
Creighton	X			
Menéndez	X			
Paxton	X			
Schwertner	X			
Whitmire	X			
Zaffirini	X			

A BILL TO BE ENTITLED
AN ACT

relating to security for state agency information and information technologies.

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

SECTION 1. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2061, and a heading is added to that chapter to read as follows:

CHAPTER 2061. INFORMATION SECURITY

SECTION 2. Chapter 2061, Government Code, as added by this Act, is amended by adding Subchapter A to read as follows:

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2061.0001. DEFINITIONS. In this chapter:

(1) "Breach of system security" has the meaning assigned by Section 521.053(a), Business & Commerce Code.

(2) "Computer," "computer network," "computer program," "computer system," and "computer software" have the meanings assigned by Section 33.01, Penal Code.

(3) "Confidential information" means information that is required to be protected from unauthorized disclosure or public release under state or federal law or a legal agreement.

(4) "Cybersecurity" means the measures taken to protect a computer or computer system against unauthorized use or access.

(5) "Data" has the meaning assigned by Section 33.01, Penal Code.

(6) "Department" means the Department of Information Resources.

(7) "Information resources" has the meaning assigned by Section 2054.003.

(8) "Information security" means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to maintain the confidentiality, integrity, and availability of the information.

(9) "Risk management" means the process of aligning information resources risk exposure with the organization's risk tolerance by accepting, transferring, or mitigating risk exposures.

(10) "Security incident" means an event that results in the accidental or deliberate unauthorized access, loss, disclosure, disruption, modification, or destruction of information or information resources.

(11) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.

(12) "State agency" has the meaning assigned by Section 2054.003.

(13) "Vulnerability" means a weakness in a system, application, or network that is subject to exploitation or misuse.

Sec. 2061.0002. GENERAL POWERS OF DEPARTMENT. (a) The department may adopt rules as necessary to implement its responsibilities under this chapter.

(b) The department may require each state agency to report to the department:

(1) each agency's use of information security and cybersecurity technologies;

(2) the effect of those technologies on the duties and functions of the agency;

(3) the costs incurred by the agency in the acquisition and use of those technologies;

(4) the procedures followed in obtaining those technologies; and

(5) other information relating to information security and cybersecurity management that in the judgment of the department should be reported.

(c) At the request of a state agency, the department may provide technical and managerial assistance relating to information security and cybersecurity management and technologies.

(d) The department may report to the governor and to the presiding officer of each house of the legislature any factors that in the opinion of the department are outside the duties of the department but that inhibit or promote effective communication about and the use of information security and cybersecurity in state government.

SECTION 3. Chapter 2061, Government Code, as added by this Act, is amended by adding Subchapter B, and a heading is added to that subchapter to read as follows:

SUBCHAPTER B. GENERAL DUTIES RELATED TO CYBERSECURITY

SECTION 4. Sections 2054.059, 2054.0591, 2054.0592, and 2054.0594, Government Code, are transferred to Subchapter B, Chapter 2061, Government Code, as added by this Act, and redesignated as Sections 2061.0051, 2061.0052, 2061.0053, and 2061.0054, Government Code, respectively, and amended to read as follows:

Sec. 2061.0051 [~~2054.059~~]. CYBERSECURITY. From available funds, the department shall:

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

(2) develop strategies and a framework for:

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

(B) cybersecurity risk assessment and mitigation planning;

(3) develop and provide training to state agencies on cybersecurity measures and awareness;

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

(5) promote public awareness of cybersecurity issues.

Sec. 2061.0052 [~~2054.0591~~]. CYBERSECURITY REPORT. (a) Not later than November 15 of each even-numbered year, the department shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity event;

(2) a review of existing statutes regarding cybersecurity and information resources technologies;

(3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity event;

(4) an evaluation of the costs and benefits of cybersecurity insurance; and

(5) an evaluation of tertiary disaster recovery options.

(b) The department or a recipient of a report under this section may redact or withhold information confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in the report in response to a request under Chapter 552 without the necessity of requesting a decision from the attorney general under Subchapter G, Chapter 552.

Sec. 2061.0053 [~~2054.0592~~]. CYBERSECURITY EMERGENCY FUNDING. If a cybersecurity event creates a need for emergency funding, the department may request that the governor or Legislative Budget Board make a proposal under Chapter 317 to provide funding to manage the operational and financial impacts from the cybersecurity event.

Sec. 2061.0054 [~~2054.0594~~]. INFORMATION SHARING AND ANALYSIS ORGANIZATION [~~CENTER~~]. (a) The department shall establish an information sharing and analysis organization [~~center~~] to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector 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 organization [~~center~~].

(c) A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information shared through the organization.

(d) A participant described by Subsection (c) may not make a voluntary disclosure under Section 552.007.

SECTION 5. Chapter 2061, Government Code, as added by this Act, is amended by adding Subchapter C, and a heading is added to that subchapter to read as follows:

SUBCHAPTER C. INFORMATION SECURITY OFFICER; INFORMATION SECURITY TRAINING AND REPORTS

SECTION 6. Section 2054.136, Government Code, is transferred to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignated as Section 2061.0101, Government Code, and amended to read as follows:

Sec. 2061.0101 [~~2054.136~~]. DESIGNATION OF [~~DESIGNATED~~] INFORMATION SECURITY OFFICER. (a) Each state agency shall designate an information security officer who:

(1) reports to the agency's executive-level management;

(2) has authority over information security for the entire agency;

(3) possesses the training and experience required to perform the duties required by department rules; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

(b) On the department's approval, two or more state agencies may jointly designate an information security officer under Subsection (a) to serve as the information security officer for each agency.

SECTION 7. Subchapter C, Chapter 2061, Government Code, as added by this Act, is amended by adding Section 2061.0102 to read as follows:

Sec. 2061.0102. INFORMATION SECURITY TRAINING. The department may provide information security training for appointed

board members, agency heads, and executive management of state agencies that is consistent with the cybersecurity awareness training provided in Section 2061.0108.

SECTION 8. Section 2054.1125, Government Code, is transferred to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignated as Section 2061.0103, Government Code, and amended to read as follows:

Sec. 2061.0103 [~~2054.1125~~]. SECURITY BREACH NOTIFICATION BY STATE AGENCY. (a) The information security officer of a [~~In this section:~~

[~~(1) "Breach of system security" has the meaning assigned by Section 521.053, Business & Commerce Code.~~

[~~(2) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.~~

[~~(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 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.

(b) Not later than the 10th business day after the date of the eradication, closure, and recovery from a breach, suspected breach, or unauthorized exposure, a state agency shall notify the department, including the chief information security officer, of the details of the event.

SECTION 9. Sections 2054.077, 2054.133, and 2054.515, Government Code, are transferred to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignated as Sections 2061.0104, 2061.0105, and 2061.0106, Government Code, respectively, and amended to read as follows:

Sec. 2061.0104 [~~2054.077~~]. VULNERABILITY REPORTS. (a) [~~In this section, a term defined by Section 33.01, Penal Code, has the meaning assigned by that section.~~

[~~(b)~~] The information security officer [~~resources manager~~] of a state agency shall 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.

(b) [~~(c)~~] Except as provided by this section, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552.

(c) [~~(d)~~] The information security officer of a state agency [~~resources manager~~] shall provide an electronic copy of the vulnerability report on its completion to:

(1) the department;

(2) the state auditor;

(3) the agency's executive director; [~~and~~]

(4) the agency's designated information resources manager; and

(5) any other information technology security oversight group specifically authorized by the legislature to

receive the report.

(d) [~~(c)~~] Separate from the executive summary described by Subsection (a) [~~(b)~~], the information security officer of a state agency 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.

Sec. 2061.0105 [~~2054.133~~]. INFORMATION SECURITY PLAN. (a) Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information.

(b) In developing the plan, the state agency shall:

(1) consider any vulnerability report prepared under Section 2061.0104 [~~2054.077~~] for the agency;

(2) incorporate the network security services provided by the department to the agency under Chapter 2059;

(3) identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;

(4) identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;

(5) include:

(A) the best practices for information security developed by the department; or

(B) a written explanation of why the best practices are not sufficient for the agency's security; and

(6) omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

(c) Not later than October 15 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the department. Subject to available resources, the department may select a portion of the submitted security plans to be assessed by the department in accordance with department rules.

(d) Each state agency's information security plan is confidential and exempt from disclosure under Chapter 552.

(e) Each state agency shall include in the agency's information security plan a written document that is signed by [~~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 and that states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan.

(f) Not later than January 13 of each odd-numbered year, the department shall submit a written report to the governor, the lieutenant governor, and the legislature evaluating information security for this state's information resources. In preparing the report, the department shall consider the information security plans submitted by state agencies under this section, any vulnerability reports submitted under Section 2061.0104 [~~2054.077~~], and other available information regarding the security of this state's information resources. The department shall omit from any written copies of the report information that could expose specific vulnerabilities in the security of this state's information resources.

Sec. 2061.0106 [~~2054.515~~]. STATE 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[~~,~~ ~~the~~] governor, the lieutenant governor, and the speaker of the house of representatives may obtain the report upon request to the department.

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

SECTION 10. Section 2054.516, Government Code, as added by Chapters 683 (H.B. 8) and 955 (S.B. 1910), Acts of the 85th Legislature, Regular Session, 2017, is reenacted, transferred to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignated as Section 2061.0107, Government Code, and amended to read as follows:

Sec. 2061.0107 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS OF STATE AGENCIES. (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 sensitive [~~personal~~] personally identifiable 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.

(b) 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.

SECTION 11. Section 2054.135, Government Code, is transferred to Subchapter C, Chapter 2061, Government Code, as added by this Act, and redesignated as Section 2061.0108, Government Code, to read as follows:

Sec. 2061.0108 [~~2054.135~~]. DATA USE AGREEMENT. (a) Each state agency shall develop a data use agreement for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the department that relate to information security standards for state agencies.

(b) A state agency shall update the data use agreement at least biennially, but may update the agreement at any time as necessary to accommodate best practices in data management.

(c) A state agency shall distribute the data use agreement developed under this section, and each update to that agreement, to employees of the agency who handle sensitive information, including financial, medical, personnel, or student data. The employee shall sign the data use agreement distributed and each update to the agreement.

(d) To the extent possible, a state agency shall provide employees described by Subsection (c) with cybersecurity awareness training to coincide with the distribution of:

(1) the data use agreement required under this section; and

(2) each biennial update to that agreement.

SECTION 12. Subchapter C, Chapter 2061, Government Code, as added by this Act, is amended by adding Section 2061.0109 to read as follows:

Sec. 2061.0109. BIENNIAL INFORMATION SECURITY REPORT. Not later than October 15 of each even-numbered year, the information security officer of each state agency shall submit an information security report for the agency. The report must include:

(1) the vulnerability report required under Section 2061.0104;

(2) the information security plan developed under Section 2061.0105;

(3) the information security assessment developed under Section 2061.0106;

(4) the data security plan for online and mobile applications required under Section 2061.0107; and

(5) the recommendations for cybersecurity and

information resources and technology security training established under Section 2061.0155.

SECTION 13. Chapter 2061, Government Code, as added by this Act, is amended by adding Subchapter D, and a heading is added to that subchapter to read as follows:

SUBCHAPTER D. STATE CYBERSECURITY AND STATE CYBERSECURITY COORDINATOR

SECTION 14. Sections 2054.511 and 2054.518, Government Code, are transferred to Subchapter D, Chapter 2061, Government Code, as added by this Act, redesignated as Sections 2061.0151 and 2061.0154, Government Code, respectively, and amended to read as follows:

Sec. 2061.0151 [~~2054.511~~]. DESIGNATION OF STATE CYBERSECURITY COORDINATOR. The executive director of the department shall designate an employee of the department as the state cybersecurity coordinator to oversee cybersecurity matters for this state.

Sec. 2061.0154 [~~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 agency personnel [~~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 agency personnel [~~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 agency personnel [~~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 15. Sections 2054.512 and 2054.513, Government Code, are transferred to Subchapter D, Chapter 2061, Government Code, as added by this Act, and redesignated as Sections 2061.0152 and 2061.0153, Government Code, respectively, to read as follows:

Sec. 2061.0152 [~~2054.512~~]. CYBERSECURITY COUNCIL. (a) The state cybersecurity coordinator shall 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.

Sec. 2061.0153 [~~2054.513~~]. CYBERSECURITY APPROVAL SEAL. The state cybersecurity coordinator may establish a voluntary program that recognizes private and public entities functioning with exemplary cybersecurity practices.

SECTION 16. Subchapter D, Chapter 2061, Government Code, as added by this Act, is amended by adding Section 2061.0155 to read as follows:

Sec. 2061.0155. RECOMMENDATIONS FOR CYBERSECURITY AND INFORMATION RESOURCES AND TECHNOLOGY SECURITY TRAINING. The department shall develop recommendations for cybersecurity and information resources and technology security training for state agency personnel and post those recommendations on the department's Internet website.

SECTION 17. Section 815.103, Government Code, is amended by adding Subsection (g) to read as follows:

(g) The retirement system shall comply with cybersecurity and information security standards established by the Department of Information Resources under Chapter 2061.

SECTION 18. Section 825.103, Government Code, is amended by amending Subsection (e) and adding Subsection (e-1) to read as follows:

(e) Except as provided by Subsection (e-1), Chapters 2054, [~~and~~] 2055, and 2061 do not apply to the retirement system. The board of trustees shall control all aspects of information technology and associated resources relating to the retirement system, including computer, data management, and telecommunication operations, procurement of hardware, software, and middleware, and telecommunication equipment and systems, location, operation, and replacement of computers, computer systems, and telecommunication systems, data processing, security, disaster recovery, and storage. The Department of Information Resources shall assist the retirement system at the request of the retirement system, and the retirement system may use any service that is available through that department.

(e-1) The retirement system shall comply with cybersecurity and information security standards established by the Department of Information Resources under Chapter 2061.

SECTION 19. The following provisions of the Government Code are repealed:

(1) Section 2054.076(b-1);

(2) Section 2054.514;

(3) Section 2054.517; and

(4) the heading to Subchapter N-1, Chapter 2054.

SECTION 20. (a) As soon as practicable after the effective date of this Act, but not later than August 31, 2020, the Department of Information Resources shall adopt rules necessary to implement the changes in law made by this Act.

(b) A rule adopted by the Department of Information Resources under Chapter 2054, Government Code, related to information security and cybersecurity continues in effect under Chapter 2061, Government Code, as added by this Act.

SECTION 21. To the extent of any conflict, this Act prevails over another Act of the 86th Legislature, Regular Session, 2019, relating to nonsubstantive additions to and corrections in enacted codes.

SECTION 22. This Act takes effect September 1, 2019.

* * * * *