

BILL ANALYSIS

Senate Research Center

S.B. 1779
By: Paxton
Business & Commerce
4/8/2019
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

As proposed, S.B. 1779 amends current law relating to security for state agency information and information technologies.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Texas Department of Information Resources (DIR) in SECTION 2 (Section 2061.0002, Government Code) of this bill.

Rulemaking authority is expressly granted to DIR in SECTION 20 of this bill.

Rulemaking authority previously granted to DIR is modified in SECTION 9 (Section 2061.0106, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

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

CHAPTER 2061. INFORMATION SECURITY

SECTION 2. Amends Chapter 2061, Government Code, as added by this Act, by adding Subchapter A, as follows:

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2061.0001. DEFINITIONS. (1) Defines "breach of system security."

(2) Defines "computer," "computer network," "computer program," "computer system," and "computer software."

(3) Defines "confidential information."

(4) Defines "cybersecurity."

(5) Defines "data."

(6) Defines "department" as the Texas Department of Information Resources (DIR).

(7) Defines "information resources."

(8) Defines "information security."

(9) Defines "risk management."

(10) Defines "security incident."

(11) Defines "sensitive personal information."

(12) Defines "state agency."

(13) Defines "vulnerability."

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

(b) Authorizes DIR to require each state agency to report to DIR:

(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 DIR should be reported.

(c) Authorizes DIR, at the request of a state agency, to provide technical and managerial assistance relating to information security and cybersecurity management and technologies.

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

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

SUBCHAPTER B. GENERAL DUTIES RELATED TO CYBERSECURITY

SECTION 4. Transfers Sections 2054.059, 2054.0591, 2054.0592, and 2054.0594, Government Code, to Subchapter B, Chapter 2061, Government Code, as added by this Act, redesignates them as Sections 2061.0051, 2061.0052, 2061.0053, and 2061.0054, Government Code, respectively, and amends them as follows:

2061.0051–2061.0053. Makes no further changes to these sections.

2061.054. New heading: INFORMATION SHARING AND ANALYSIS ORGANIZATION. (a) Requires DIR to establish an information sharing and analysis organization 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, rather than 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) Creates this subsection from existing Subsection (c) and requires DIR to provide administrative support to the information sharing and analysis organization, rather than requiring DIR, using funds other than funds appropriated to DIR in a general appropriations act, to provide administrative support to the information sharing and analysis center. Deletes existing text requiring DIR to

appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) Requires a participant in the information sharing and analysis organization to assert any exception available under state or federal law, including Section 552.139 (Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers), in response to a request for public disclosure of information shared through the organization.

(d) Prohibits a participant described by Subsection (c) from making a voluntary disclosure under Section 552.007 (Voluntary Disclosure of Certain Information When Disclosure Not Required).

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

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

SECTION 6. Transfers Section 2054.136, Government Code, to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignates it as Section 2061.0101, Government Code, and amends it as follows:

Sec. 2061.0101. New heading: DESIGNATION OF INFORMATION SECURITY OFFICER. (a) Creates this subsection from existing text and makes no further changes to this subsection.

(b) Authorizes two or more state agencies, on DIR's approval, to jointly designate an information security officer under Subsection (a) (relating to requiring each state agency to designate an information security officer and the requirements, powers, and duties of the information security officer) to serve as the information security officer for each agency.

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

Sec. 2061.0102. INFORMATION SECURITY TRAINING. Authorizes DIR to 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. Transfers Section 2054.1125, Government Code, to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignates it as Section 2061.0103, Government Code, and amends it as follows:

Sec. 2061.0103. SECURITY BREACH NOTIFICATION BY STATE AGENCY. (a) Deletes existing text defining "breach of system security" and "sensitive personal information" and creates this subsection from existing Subsection (b). Requires the information security officer of 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, rather than requiring 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, to, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) makes no further changes to this subdivision; and

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

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

(B) makes no further changes to this paragraph.

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

SECTION 9. Transfers Sections 2054.077, 2054.133, and 2054.515, Government Code, to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignates them as Sections 2061.0104, 2061.0105, and 2061.0106, Government Code, respectively, and amends them as follows:

Sec. 2061.0104. VULNERABILITY REPORTS. (a) Deletes existing text providing that, in this section, a term defined by Section 33.01 (Definitions), Penal Code, has the meaning assigned by that section, creates this subsection from existing Subsection (b), and reletters subsequent subsections accordingly. Requires the information security officer of a state agency, rather than the information resources manager of a state agency, to prepare or have prepared a certain report.

(b) Makes no further changes to this subsection.

(c) Requires the information security officer of a state agency, rather than the information resources manager, to provide an electronic copy of the vulnerability report on its completion to:

(1) and (2) makes no further changes to these subdivisions;

(3) makes a nonsubstantive change;

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

(5) creates this subdivision from existing text.

(d) Requires the information security officer of a state agency, separate from the executive summary described by Subsection (a), rather than requiring a state agency, separate from the executive summary described by Subsection (b), to prepare a summary of the agency's vulnerability report that does not contain certain information.

Sec. 2061.0105. INFORMATION SECURITY PLAN. (a) Makes no changes to this subsection.

(b) Makes a conforming change to this subsection.

(c) and (d) Makes no changes to these subsections.

(e) Requires each state agency to include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager 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, rather than a written acknowledgement 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.

(f) Makes a conforming change to this subsection.

Sec. 2061.0106. New heading: STATE AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) Makes no changes to this subsection.

(b) Requires a state agency, not later than December 1 of the year in which the state agency conducts the assessment under Subsection (a) (relating to requiring each state agency, at least once every two years, to conduct an information security assessment of certain systems, security measures, and vulnerabilities), to report the results of the assessment to DIR, rather than requiring a state agency, not later than December 1 of the year in which the state agency conducts the assessment under Subsection (a), to report the results of the assessment to DIR, the governor, the lieutenant governor, and the speaker of the house of representatives. Authorizes the governor, the lieutenant governor, and the speaker of the house of representatives to obtain the report upon request to DIR.

(c) Requires DIR by rule, rather than authorizing DIR by rule, to establish the requirements for the information security assessment and report required by this section.

SECTION 10. Reenacts 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, transfers it to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignates it as Section 2061.0107, Government Code, and amends it as follows:

Sec. 2061.0107. New heading: DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS OF STATE AGENCIES. (a) Requires each state agency implementing an Internet website or mobile application that processes any sensitive personally identifiable information or confidential information to take certain actions, rather than requiring each state agency, other than an institution of higher education subject to Section 2054.517 (Data Security Procedures for Online and Mobile Applications of Institutions of Higher Education), implementing an Internet website or mobile application that processes any sensitive personal personally identifiable information or confidential information to take certain actions.

(b) Makes no further changes to this subsection.

SECTION 11. Transfers Section 2054.135, Government Code, to Subchapter C, Chapter 2061, Government Code, as added by this Act, redesignates it as Section 2061.0108, Government Code, and makes no further changes to it.

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

Sec. 2061.0109. BIENNIAL INFORMATION SECURITY REPORT. Requires the information security officer of each state agency, not later than October 15 of each even-numbered year, to submit an information security report for the agency. Requires the report to 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. Amends Chapter 2061, Government Code, as added by this Act, by adding Subchapter D, and adds a heading to that subchapter to read as follows:

SUBCHAPTER D. STATE CYBERSECURITY AND STATE CYBERSECURITY
COORDINATOR

SECTION 14. Transfers Sections 2054.511 and 2054.518, Government Code, to Subchapter D, Chapter 2061, Government Code, as added by this Act, redesignates them as Sections 2061.0151 and 2061.0154, Government Code, respectively, and amends them as follows:

Sec. 2061.0151. New heading: DESIGNATION OF STATE CYBERSECURITY COORDINATOR. Makes a nonsubstantive change.

Sec. 2061.0154. CYBERSECURITY RISKS AND INCIDENTS. (a) Authorizes the authorized agreement between DIR and a national organization to support certain efforts of DIR to include provisions for:

(1) providing fee reimbursement for appropriate industry-recognized certification examinations for and training to state agency personnel preparing for and responding to cybersecurity risks and incidents, rather than examinations for and training to state agencies preparing for and responding to cybersecurity risks and incidents;

(2) makes a conforming change;

(3) and (4) makes no further changes to these subdivisions;

(5) makes a conforming change; and

(6) and (7) makes no further changes to these subdivisions.

SECTION 15. Transfers Sections 2054.512 and 2054.513, Government Code, to Subchapter D, Chapter 2061, Government Code, as added by this Act, redesignates them as Sections 2061.0152 and 2061.0153, Government Code, respectively, and makes no further changes to these sections.

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

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

SECTION 17. Amends Section 815.103, Government Code, by adding Subsection (g), to require the Employees Retirement System of Texas to comply with cybersecurity and information security standards established by DIR under Chapter 2061.

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

(e) Provides that, except as provided by Subsection (e-1), Chapters 2054 (Information Resources), 2055 (Electronic Grant System), and 2061, rather than Chapters 2054 and 2055, do not apply to the Teacher Retirement System of Texas.

(e-1) Requires the Teacher Retirement System of Texas to comply with cybersecurity and information security standards established by DIR under Chapter 2061.

SECTION 19. Repealer: Section 2054.076(b-1) (relating to requiring DIR to provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training that are required to be completed by all information resources employees of the agencies), Government Code.

Repealer: Section 2054.514 (Recommendations), Government Code.

Repealer: Section 2054.517 (Data Security Procedures for Online and Mobile Applications of Institutions of Higher Education), Government Code.

Repealer: the heading to Subchapter N-1 (State Cybersecurity), Chapter 2054, Government Code.

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

(b) Provides that a rule adopted by DIR 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. Provides that, 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. Effective date: September 1, 2019.