BILL ANALYSIS

Senate Research Center
86R20251 AAF/GRM-F

C.S.S.B. 64
By: Nelson
Business & Commerce
4/13/2019
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The Texas Cybersecurity Act, (H.B. 8, 85R) made sweeping improvements to assess and improve the state's cybersecurity posture. H.B. 8 also created the Senate Select Committee on Cybersecurity. Hearings conducted during the interim identified several areas where the State could benefit from improvements.

S.B. 64 seeks to address those issues by improving Texas' cybersecurity to protect data and ensure that key services are delivered by strengthening state oversight of cybersecurity, bolstering the cyber workforce, assisting local government recovering from cyber events, and improving oversight of the electric grid. (Original Author's/Sponsor's Statement of Intent)

C.S.S.B. 64 amends current law relating to cybersecurity for information resources.

RULEMAKING AUTHORITY

Rulemaking authority previously granted to the Department of Information Resources is rescinded in SECTION 19 (Section 2054.119, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter C, Chapter 61, Education Code, by adding Section 61.09091, as follows:

> Sec. 61.09091. STRATEGIES TO INCENTIVIZE CYBERSECURITY DEGREE PROGRAMS. (a) Requires the Texas Higher Education Coordinating Board (THECB) in collaboration with the Department of Information Resources (DIR) to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity.
>
> (b) Requires THECB to consult with institutions of higher education as necessary to carry out its duties under this section.
>
> (c) Requires THECB, not later than September 1, 2020, to submit a written report detailing the strategies identified under this section to the lieutenant governor, the speaker of the house of representatives, the presiding officer of each legislative standing committee with primary jurisdiction over higher education, and each governing board of an institution of higher education.
>
> (d) Provides that this section expires September 1, 2021.

SECTION 2. Amends Section 418.004(1), Government Code, to redefine "disaster" to include a cybersecurity event.

SECTION 3. 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 2054 (Information Resources).

SECTION 4. 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 and 2055 (Electronic Grant System) do not apply to the Teacher Retirement System of Texas (TRS).

(e-1) Requires TRS to comply with cybersecurity and information security standards established by DIR under Chapter 2054.

SECTION 5. Amends Section 2054.0075, Government Code, as follows:

Sec. 2054.0075. EXCEPTION: PUBLIC JUNIOR COLLEGE. Provides that this chapter does not apply to a public junior college or a public junior college district, except as necessary to comply with information security standards and for participation in shared technology services, including the electronic government project implemented under Subchapter I (State Electronic Internet Portal Project) and statewide technology centers under Subchapter L (Statewide Technology Centers). Deletes existing text creating an exception under Section 2054.119 (Bids or Proposals For Interagency Contracts), Government Code.

SECTION 6. Amends Section 2054.0591(a), Government Code, as follows:

(a) Requires the report relating to preventive and recovery efforts the state can undertake to improve cybersecurity to include:

(1)–(2) makes no changes to these subdivisions;

(3) makes a nonsubstantive change to this subdivision; and

(4) an evaluation of a program that provides an information security officer to assist small state agencies and local governments that are unable to justify hiring a full-time information security officer, rather than an evaluation of the costs and benefits of cybersecurity insurance.

Deletes existing Subdivision (5) relating to an evaluation of tertiary disaster recovery options.

SECTION 7. Amends Section 2054.0594, Government Code, as follows:

Sec. 2054.0594. New heading: INFORMATION SHARING AND ANALYSIS ORGANIZATION. (a) Requires DIR to establish an information sharing and analysis organization, rather than center, to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector, rather than for state agencies, to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) Deletes existing text requiring DIR to appoint representatives to the center. Requires DIR to provide administrative support to the information sharing and analysis organization. Redesignates existing Subsection (c) as this subsection, deletes existing text relating to the use of funds other than funds appropriated to DIR in a general appropriations act, and makes a conforming change.

(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. Provides that Section 552.007 (Voluntary Disclosure of Certain Information When Disclosure Not Required) does not apply to information described by this subsection.

SECTION 8. Amends Section 2054.068(e), Government Code, as follows:

(e) Requires the consolidated report required by Subsection (d) to:

(1) makes no changes to this subdivision; and

(2) for a state agency found to be at higher security and operational risks, include a detailed analysis of agency efforts to address the risks and related vulnerabilities. Deletes existing text relating to an estimate of the costs to implement and agency requirements to address risk and related vulnerabilities.

SECTION 9. Amends Subchapter C, Chapter 2054, Government Code, by adding Section 2054.069, as follows:

Sec. 2054.069. PRIORITIZED CYBERSECURITY AND LEGACY SYSTEM PROJECTS REPORT. (a) Requires DIR, not later than October 1 of each even-numbered year, to submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects, and state agency projects to modernize or replace legacy systems, as defined by Section 2054.571 (Definition).

(b) Requires each state agency to coordinate with DIR to implement this section.

(c) Requires a state agency to assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information contained in or written, produced, collected, assembled, or maintained in connection with the report under Subsection (a). Provides that Section 552.007 does not apply to information described by this subsection.

SECTION 10. Amends Sections 2054.077(b) and (d), Government Code, as follows:

(b) Requires the information security officer, rather than the information resources manager, of a state agency to prepare or have prepared a report, including certain information related to device vulnerability.

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

(1)–(3) makes no changes to these subdivisions;

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

(5) creates this subdivision from existing Subdivision (4) and makes no further changes.

SECTION 11. Amends Section 2054.1125, Government Code, by amending Subsection (b) and adding Subsection (c), as follows:

(b) Deletes existing requirement that the state cybersecurity coordinator be notified not later than 48 hours after the discovery of a breach, suspected breach, or unauthorized exposure.

(c) 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 and include in the notification an analysis of the cause of the event.

SECTION 12. Amends Section 2054.133(e), Government Code, as follows:

(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 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 acknowledgment that the executive director or other head of agency, the chief financial officer, and each manager as designated by the state agency have been made aware of such risks.

SECTION 13. 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, and amends it to delete existing text exempting an institution of higher education subject to Section 2054.517 (Data Security Procedures For Online and Mobile Applications of Institutions of Higher Education) from certain cybersecurity requirements and to make a nonsubstantive change.

SECTION 14. Amends Section 2059.058(b), Government Code, to add a public junior college to a list of entities to which DIR is authorized to provide network security by agreement.

SECTION 15. Amends Section 1702.104, Occupations Code, by adding Subsection (c) to provide that the review and analysis of computer-based data for the purpose of preparing for or responding to a cybersecurity event does not constitute an investigation for purposes of this section (Investigations Company) and does not require licensing under this chapter (Private Security).

SECTION 16. Amends Chapter 31, Utilities Code, by designating Sections 31.001 through 31.005 as Subchapter A and adding a subchapter heading to read as follows:

SUBCHAPTER A. GENERAL PROVISIONS

SECTION 17. Amends Chapter 31, Utilities Code, by adding Subchapter B, as follows:

SUBCHAPTER B. CYBERSECURITY

Sec. 31.051. DEFINITION. Defines "utility."

Sec. 31.052. CYBERSECURITY COORDINATION PROGRAM FOR UTILITIES. (a) Requires the Public Utility Commission of Texas (PUC) to establish a program to monitor cybersecurity efforts among utilities in this state. Requires the program to:

(1) provide guidance on best practices in cybersecurity and facilitate the sharing of cybersecurity information between utilities; and

(2) provide guidance on best practices for cybersecurity controls for supply chain risk management of cybersecurity systems used by utilities, which may include, as applicable, best practices related to:

(A) software integrity and authenticity;

(B) vendor risk management and procurement controls, including notification by vendors of incidents related to the vendor's products and services; and

(C) vendor remote access.

(b) Authorizes the PUC to collaborate with the state cybersecurity coordinator and the cybersecurity council established under Chapter 2054, Government Code, in implementing the program.

SECTION 18. Amends Section 39.151, Utilities Code, by adding Subsections (o) and (p), as follows:

(o) Requires an independent organization certified by the PUC under this section to:

(1) conduct internal cybersecurity risk assessment, vulnerability testing, and employee training to the extent the independent organization is not otherwise required to do so under applicable state and federal cybersecurity and information laws; and

(2) submit a report annually to the PUC on the independent organization's compliance with applicable cybersecurity and information security laws.

(p) Provides that information submitted in a report under Subsection (o) is confidential and not subject to disclosure under Chapter 552 (Public Information), Government Code.

SECTION 19. Repealer: Section 2054.119 (Bids or Proposals For Interagency Contracts), Government Code.

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

SECTION 20. 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 and corrections in enacted codes.

SECTION 21. Effective date: September 1, 2019.