

By: Nelson
(Phelan)

S.B. No. 64

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for information resources.

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

SECTION 1. Subchapter C, Chapter 61, Education Code, is amended by adding Section 61.09091 to read as follows:

Sec. 61.09091. STRATEGIES TO INCENTIVIZE CYBERSECURITY DEGREE PROGRAMS. (a) The board in collaboration with the Department of Information Resources shall identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity.

(b) The board shall consult with institutions of higher education as necessary to carry out its duties under this section.

(c) Not later than September 1, 2020, the board shall 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) This section expires September 1, 2021.

SECTION 2. Section 418.004(1), Government Code, is amended to read as follows:

(1) "Disaster" means the occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property

1 resulting from any natural or man-made cause, including fire,
2 flood, earthquake, wind, storm, wave action, oil spill or other
3 water contamination, volcanic activity, epidemic, air
4 contamination, blight, drought, infestation, explosion, riot,
5 hostile military or paramilitary action, extreme heat,
6 cybersecurity event, other public calamity requiring emergency
7 action, or energy emergency.

8 SECTION 3. Section [815.103](#), Government Code, is amended by
9 adding Subsection (g) to read as follows:

10 (g) The retirement system shall comply with cybersecurity
11 and information security standards established by the Department of
12 Information Resources under Chapter [2054](#).

13 SECTION 4. Section [825.103](#), Government Code, is amended by
14 amending Subsection (e) and adding Subsection (e-1) to read as
15 follows:

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

1 that department.

2 (e-1) The retirement system shall comply with cybersecurity
3 and information security standards established by the Department of
4 Information Resources under Chapter 2054.

5 SECTION 5. Section 2054.0075, Government Code, is amended
6 to read as follows:

7 Sec. 2054.0075. EXCEPTION: PUBLIC JUNIOR COLLEGE. This
8 chapter does not apply to a public junior college or a public junior
9 college district, except as necessary to comply with information
10 security standards and for participation in shared technology
11 services, including the electronic government project implemented
12 under Subchapter I and statewide technology centers under
13 Subchapter L [~~except as to Section 2054.119, Government Code~~].

14 SECTION 6. Section 2054.0591(a), Government Code, is
15 amended to read as follows:

16 (a) Not later than November 15 of each even-numbered year,
17 the department shall submit to the governor, the lieutenant
18 governor, the speaker of the house of representatives, and the
19 standing committee of each house of the legislature with primary
20 jurisdiction over state government operations a report identifying
21 preventive and recovery efforts the state can undertake to improve
22 cybersecurity in this state. The report must include:

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

26 (2) a review of existing statutes regarding
27 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; 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 ~~[the costs and benefits of cybersecurity insurance; and~~

~~(5) an evaluation of tertiary disaster recovery options]~~.

SECTION 7. Section 2054.0594, Government Code, is amended to read as follows:

Sec. 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

1 organization shall assert any exception available under state or
2 federal law, including Section 552.139, in response to a request
3 for public disclosure of information shared through the
4 organization. Section 552.007 does not apply to information
5 described by this subsection.

6 SECTION 8. Section 2054.068(e), Government Code, is amended
7 to read as follows:

8 (e) The consolidated report required by Subsection (d)
9 must:

10 (1) include an analysis and assessment of each state
11 agency's security and operational risks; and

12 (2) for a state agency found to be at higher security
13 and operational risks, include a detailed analysis of agency
14 efforts to address the risks and related vulnerabilities~~[, and an~~
15 ~~estimate of the costs to implement, the:~~

16 [~~(A) requirements for the agency to address the~~
17 ~~risks and related vulnerabilities, and~~

18 [~~(B) agency's efforts to address the risks~~
19 ~~through the:~~

20 [~~(i) modernization of information~~
21 ~~technology systems,~~

22 [~~(ii) use of cloud services, and~~

23 [~~(iii) use of a statewide technology center~~
24 ~~established by the department]~~.

25 SECTION 9. Subchapter C, Chapter 2054, Government Code, is
26 amended by adding Section 2054.069 to read as follows:

27 Sec. 2054.069. PRIORITIZED CYBERSECURITY AND LEGACY SYSTEM

1 PROJECTS REPORT. (a) Not later than October 1 of each
2 even-numbered year, the department shall submit a report to the
3 Legislative Budget Board that prioritizes, for the purpose of
4 receiving funding, state agency:

5 (1) cybersecurity projects; and
6 (2) projects to modernize or replace legacy systems,
7 as defined by Section 2054.571.

8 (b) Each state agency shall coordinate with the department
9 to implement this section.

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

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

18 (b) The information security officer [~~resources manager~~] of
19 a state agency shall prepare or have prepared a report, including an
20 executive summary of the findings of the biennial report, not later
21 than October 15 of each even-numbered year, assessing the extent to
22 which a computer, a computer program, a computer network, a
23 computer system, a printer, an interface to a computer system,
24 including mobile and peripheral devices, computer software, or data
25 processing of the agency or of a contractor of the agency is
26 vulnerable to unauthorized access or harm, including the extent to
27 which the agency's or contractor's electronically stored

information is vulnerable to alteration, damage, erasure, or inappropriate use.

(d) The information security officer [~~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;
- (4) the agency's designated information resources manager; and

(5) [~~(4)~~] any other information technology security oversight group specifically authorized by the legislature to receive the report.

SECTION 11. Section 2054.1125, Government Code, is amended by amending Subsection (b) and adding Subsection (c) 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 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

1 information security officer [~~and the state cybersecurity~~
2 ~~coordinator~~]; or

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

6 (c) Not later than the 10th business day after the date of
7 the eradication, closure, and recovery from a breach, suspected
8 breach, or unauthorized exposure, a state agency shall notify the
9 department, including the chief information security officer, of
10 the details of the event and include in the notification an analysis
11 of the cause of the event.

12 SECTION 12. Section 2054.133(e), Government Code, is
13 amended to read as follows:

14 (e) Each state agency shall include in the agency's
15 information security plan a written document that is signed by
16 ~~[acknowledgment that]~~ the ~~[executive director or other]~~ head of the
17 agency, the chief financial officer, and each executive manager
18 ~~[as]~~ designated by the state agency and states that those persons
19 have been made aware of the risks revealed during the preparation of
20 the agency's information security plan.

21 SECTION 13. Section 2054.516, Government Code, as added by
22 Chapters 683 (H.B. 8) and 955 (S.B. 1910), Acts of the 85th
23 Legislature, Regular Session, 2017, is reenacted and amended to
24 read as follows:

25 Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE
26 APPLICATIONS. (a) Each state agency~~[, other than an institution~~
27 ~~of higher education subject to Section 2054.517,~~] implementing an

Internet website or mobile application that processes any sensitive personal or 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 14. Section 2059.058(b), Government Code, is amended to read as follows:

(b) In addition to the department's duty to provide network security services to state agencies under this chapter, the department by agreement may provide network security to:

(1) each house of the legislature;

(2) an agency that is not a state agency, including a legislative agency;

(3) a political subdivision of this state, including a county, municipality, or special district; ~~and~~

(4) an independent organization, as defined by Section 39.151, Utilities Code; and

(5) a public junior college.

SECTION 15. Section 1702.104, Occupations Code, is amended

by adding Subsection (c) to read as follows:

(c) 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 and does not require licensing under this chapter.

SECTION 16. Chapter 31, Utilities Code, is amended 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. Chapter 31, Utilities Code, is amended by adding Subchapter B to read as follows:

SUBCHAPTER B. CYBERSECURITY

Sec. 31.051. DEFINITION. In this subchapter, "utility" means:

- (1) an electric cooperative;
- (2) an electric utility;
- (3) a municipally owned electric utility;
- (4) a retail electric provider; or
- (5) a transmission and distribution utility.

Sec. 31.052. CYBERSECURITY COORDINATION PROGRAM FOR UTILITIES. (a) The commission shall establish a program to monitor cybersecurity efforts among utilities in this state. The program shall:

- (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) The commission may collaborate with the state
cybersecurity coordinator and the cybersecurity council
established under Chapter 2054, Government Code, in implementing
the program.

SECTION 18. Section 39.151, Utilities Code, is amended by
adding Subsections (o) and (p) to read as follows:

(o) An independent organization certified by the commission
under this section shall:

(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
security laws; and

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

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

1 SECTION 19. Sections 2054.119 and 2054.517, Government
2 Code, are repealed.

3 SECTION 20. To the extent of any conflict, this Act prevails
4 over another Act of the 86th Legislature, Regular Session, 2019,
5 relating to nonsubstantive additions and corrections in enacted
6 codes.

7 SECTION 21. This Act takes effect September 1, 2019.