

By: Paxton
(Parker)

S.B. No. 1779

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,

1 Penal Code.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 SUBCHAPTER B. GENERAL DUTIES RELATED TO CYBERSECURITY

1 SECTION 4. Sections [2054.059](#), [2054.0591](#), [2054.0592](#), and
2 [2054.0594](#), Government Code, are transferred to Subchapter B,
3 Chapter 2061, Government Code, as added by this Act, and
4 redesignated as Sections 2061.0051, 2061.0052, 2061.0053, and
5 2061.0054, Government Code, respectively, and amended to read as
6 follows:

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

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

12 (2) develop strategies and a framework for:

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

15 (B) cybersecurity risk assessment and mitigation
16 planning;

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

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

22 (5) promote public awareness of cybersecurity issues.

23 Sec. 2061.0052 [~~2054.0591~~]. CYBERSECURITY REPORT.

24 (a) Not later than November 15 of each even-numbered year, the
25 department shall submit to the governor, the lieutenant governor,
26 the speaker of the house of representatives, and the standing
27 committee of each house of the legislature with primary

1 jurisdiction over state government operations a report identifying
2 preventive and recovery efforts the state can undertake to improve
3 cybersecurity in this state. The report must include:

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

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

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

12 (4) an evaluation of a program that provides an
13 information security officer to assist small state agencies and
14 local governments that are unable to justify hiring a full-time
15 information security officer [~~the costs and benefits of~~
16 ~~cybersecurity insurance, and~~

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

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

25 Sec. 2061.0053 [~~2054.0592~~]. CYBERSECURITY EMERGENCY
26 FUNDING. If a cybersecurity event creates a need for emergency
27 funding, the department may request that the governor or

1 Legislative Budget Board make a proposal under Chapter 317 to
2 provide funding to manage the operational and financial impacts
3 from the cybersecurity event.

4 Sec. 2061.0054 [~~2054.0594~~]. INFORMATION SHARING AND
5 ANALYSIS ORGANIZATION [~~CENTER~~]. (a) The department shall
6 establish an information sharing and analysis organization
7 [~~center~~] to provide a forum for state agencies, local governments,
8 public and private institutions of higher education, and the
9 private sector to share information regarding cybersecurity
10 threats, best practices, and remediation strategies.

11 (b) [~~The department shall appoint persons from appropriate~~
12 ~~state agencies to serve as representatives to the information~~
13 ~~sharing and analysis center.~~

14 [~~(c)~~] The department [~~, using funds other than funds~~
15 ~~appropriated to the department in a general appropriations act,~~]
16 shall provide administrative support to the information sharing and
17 analysis organization [~~center~~].

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

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

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

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

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

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

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

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

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

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

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

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

25 Sec. 2061.0102. INFORMATION SECURITY TRAINING. The
26 department may provide information security training for appointed
27 board members, agency heads, and executive management of state

1 agencies that is consistent with the cybersecurity awareness
2 training provided in Section 2061.0108.

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

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

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

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

14 [~~(b) A~~] state agency that owns, licenses, or maintains
15 computerized data that includes sensitive personal information,
16 confidential information, or information the disclosure of which is
17 regulated by law shall, in the event of a breach or suspected breach
18 of system security or an unauthorized exposure of that information:

19 (1) comply with the notification requirements of
20 Section 521.053, Business & Commerce Code, to the same extent as a
21 person who conducts business in this state; and

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

24 (A) the department, including the chief
25 information security officer [~~and the state cybersecurity~~
26 ~~coordinator~~]; or

27 (B) if the breach, suspected breach, or

1 unauthorized exposure involves election data, the secretary of
2 state.

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

8 SECTION 9. Sections 2054.077, 2054.133, and 2054.515,
9 Government Code, are transferred to Subchapter C, Chapter 2061,
10 Government Code, as added by this Act, redesignated as Sections
11 2061.0104, 2061.0105, and 2061.0106, Government Code,
12 respectively, and amended to read as follows:

13 Sec. 2061.0104 [~~2054.077~~]. VULNERABILITY REPORTS.

14 (a) [~~In this section, a term defined by Section 33.01, Penal Code,~~
15 ~~has the meaning assigned by that section.~~

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

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

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

- 8 (1) the department;
- 9 (2) the state auditor;
- 10 (3) the agency's executive director; [~~and~~]
- 11 (4) the agency's designated information resources
12 manager; and
- 13 (5) any other information technology security
14 oversight group specifically authorized by the legislature to
15 receive the report.

16 (d) [~~(e)~~] Separate from the executive summary described by
17 Subsection (a) [~~(b)~~], the information security officer of a state
18 agency shall prepare a summary of the agency's vulnerability report
19 that does not contain any information the release of which might
20 compromise the security of the state agency's or state agency
21 contractor's computers, computer programs, computer networks,
22 computer systems, printers, interfaces to computer systems,
23 including mobile and peripheral devices, computer software, data
24 processing, or electronically stored information. The summary is
25 available to the public on request.

26 Sec. 2061.0105 [~~2054.133~~]. INFORMATION SECURITY PLAN.

27 (a) Each state agency shall develop, and periodically update, an

1 information security plan for protecting the security of the
2 agency's information.

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

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

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

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

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

14 (5) include:

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

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

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

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

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

3 (e) Each state agency shall include in the agency's
4 information security plan a written document that is signed by
5 ~~[acknowledgment that]~~ the ~~[executive director or other]~~ head of the
6 agency, the chief financial officer, and each executive manager
7 ~~[as]~~ designated by the state agency and that states that those
8 persons have been made aware of the risks revealed during the
9 preparation of the agency's information security plan.

10 (f) Not later than January 13 of each odd-numbered year, the
11 department shall submit a written report to the governor, the
12 lieutenant governor, and the legislature evaluating information
13 security for this state's information resources. In preparing the
14 report, the department shall consider the information security
15 plans submitted by state agencies under this section, any
16 vulnerability reports submitted under Section 2061.0104
17 ~~[2054.077]~~, and other available information regarding the security
18 of this state's information resources. The department shall omit
19 from any written copies of the report information that could expose
20 specific vulnerabilities in the security of this state's
21 information resources.

22 Sec. 2061.0106 ~~[2054.515]~~. STATE AGENCY INFORMATION
23 SECURITY ASSESSMENT AND REPORT. (a) At least once every two
24 years, each state agency shall conduct an information security
25 assessment of the agency's information resources systems, network
26 systems, digital data storage systems, digital data security
27 measures, and information resources vulnerabilities.

1 (b) Not later than December 1 of the year in which a state
2 agency conducts the assessment under Subsection (a), the agency
3 shall report the results of the assessment to the department. The~~[~~
4 ~~the]~~ governor, the lieutenant governor, and the speaker of the
5 house of representatives may obtain the report upon request to the
6 department.

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

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

16 Sec. 2061.0107 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE
17 AND MOBILE APPLICATIONS OF STATE AGENCIES. (a) Each state
18 agency~~[, other than an institution of higher education subject to~~
19 ~~Section 2054.517,~~] implementing an Internet website or mobile
20 application that processes any sensitive ~~[personal]~~ personally
21 identifiable information or confidential information must:

22 (1) submit a biennial data security plan to the
23 department not later than October 15 of each even-numbered year to
24 establish planned beta testing for the website or application; and

25 (2) subject the website or application to a
26 vulnerability and penetration test and address any vulnerability
27 identified in the test.

1 (b) The department shall review each data security plan
2 submitted under Subsection (a) and make any recommendations for
3 changes to the plan to the state agency as soon as practicable after
4 the department reviews the plan.

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

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

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

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

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

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

1 (2) each biennial update to that agreement.

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

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

9 (1) the vulnerability report required under Section
10 2061.0104;

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

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

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

17 (5) the recommendations for cybersecurity and
18 information resources and technology security training established
19 under Section 2061.0155.

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

23 SUBCHAPTER D. STATE CYBERSECURITY AND STATE CYBERSECURITY

24 COORDINATOR

25 SECTION 14. Sections 2054.511 and 2054.518, Government
26 Code, are transferred to Subchapter D, Chapter 2061, Government
27 Code, as added by this Act, redesignated as Sections 2061.0151 and

1 2061.0154, Government Code, respectively, and amended to read as
2 follows:

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

8 Sec. 2061.0154 [~~2054.518~~]. CYBERSECURITY RISKS AND
9 INCIDENTS. (a) The department shall develop a plan to address
10 cybersecurity risks and incidents in this state. The department
11 may enter into an agreement with a national organization, including
12 the National Cybersecurity Preparedness Consortium, to support the
13 department's efforts in implementing the components of the plan for
14 which the department lacks resources to address internally. The
15 agreement may include provisions for:

16 (1) providing fee reimbursement for appropriate
17 industry-recognized certification examinations for and training to
18 state agency personnel [~~agencies~~] preparing for and responding to
19 cybersecurity risks and incidents;

20 (2) developing and maintaining a cybersecurity risks
21 and incidents curriculum using existing programs and models for
22 training state agency personnel [~~agencies~~];

23 (3) delivering to state agency personnel with access
24 to state agency networks routine training related to appropriately
25 protecting and maintaining information technology systems and
26 devices, implementing cybersecurity best practices, and mitigating
27 cybersecurity risks and vulnerabilities;

1 (4) providing technical assistance services to
2 support preparedness for and response to cybersecurity risks and
3 incidents;

4 (5) conducting cybersecurity training and simulation
5 exercises for state agency personnel [~~agencies~~] to encourage
6 coordination in defending against and responding to cybersecurity
7 risks and incidents;

8 (6) assisting state agencies in developing
9 cybersecurity information-sharing programs to disseminate
10 information related to cybersecurity risks and incidents; and

11 (7) incorporating cybersecurity risk and incident
12 prevention and response methods into existing state emergency
13 plans, including continuity of operation plans and incident
14 response plans.

15 (b) In implementing the provisions of the agreement
16 prescribed by Subsection (a), the department shall seek to prevent
17 unnecessary duplication of existing programs or efforts of the
18 department or another state agency.

19 (c) In selecting an organization under Subsection (a), the
20 department shall consider the organization's previous experience
21 in conducting cybersecurity training and exercises for state
22 agencies and political subdivisions.

23 (d) The department shall consult with institutions of
24 higher education in this state when appropriate based on an
25 institution's expertise in addressing specific cybersecurity risks
26 and incidents.

27 SECTION 15. Sections [2054.512](#) and [2054.513](#), Government

1 Code, are transferred to Subchapter D, Chapter 2061, Government
2 Code, as added by this Act, and redesignated as Sections 2061.0152
3 and 2061.0153, Government Code, respectively, to read as follows:

4 Sec. 2061.0152 [~~2054.512~~]. CYBERSECURITY COUNCIL.

5 (a) The state cybersecurity coordinator shall establish and lead a
6 cybersecurity council that includes public and private sector
7 leaders and cybersecurity practitioners to collaborate on matters
8 of cybersecurity concerning this state.

9 (b) The cybersecurity council must include:

10 (1) one member who is an employee of the office of the
11 governor;

12 (2) one member of the senate appointed by the
13 lieutenant governor;

14 (3) one member of the house of representatives
15 appointed by the speaker of the house of representatives; and

16 (4) additional members appointed by the state
17 cybersecurity coordinator, including representatives of
18 institutions of higher education and private sector leaders.

19 (c) In appointing representatives from institutions of
20 higher education to the cybersecurity council, the state
21 cybersecurity coordinator shall consider appointing members of the
22 Information Technology Council for Higher Education.

23 (d) The cybersecurity council shall:

24 (1) consider the costs and benefits of establishing a
25 computer emergency readiness team to address cyber attacks
26 occurring in this state during routine and emergency situations;

27 (2) establish criteria and priorities for addressing

1 cybersecurity threats to critical state installations;

2 (3) consolidate and synthesize best practices to
3 assist state agencies in understanding and implementing
4 cybersecurity measures that are most beneficial to this state; and

5 (4) assess the knowledge, skills, and capabilities of
6 the existing information technology and cybersecurity workforce to
7 mitigate and respond to cyber threats and develop recommendations
8 for addressing immediate workforce deficiencies and ensuring a
9 long-term pool of qualified applicants.

10 (e) The cybersecurity council shall provide recommendations
11 to the legislature on any legislation necessary to implement
12 cybersecurity best practices and remediation strategies for this
13 state.

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

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

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

27 SECTION 17. Section 815.103, Government Code, is amended by

1 adding Subsection (g) to read as follows:

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

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

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

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

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

- 26 (1) Section 2054.076(b-1);
27 (2) Section 2054.514;

1 (3) Section 2054.517; and

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

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

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

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

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