

By: Paxton

S.B. No. 1204

A BILL TO BE ENTITLED

AN ACT

relating to state and local government information technology infrastructure, information security, and data breach and exposure reporting.

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

SECTION 1. The heading to Section 2054.0594, Government Code, is amended to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS ORGANIZATIONS ~~[ORGANIZATION]~~.

SECTION 2. Section 2054.0594, Government Code, is amended by amending Subsections (a), (b), and (c) and adding Subsection (a-1) to read as follows:

(a) The department shall establish an intrastate 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 entities in this state to share information regarding cybersecurity threats, best practices, and remediation strategies.

(a-1) The department may establish an interstate information sharing and analysis organization to provide a forum for states to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) The department shall provide administrative support to each ~~[the]~~ information sharing and analysis organization

1 established under this section.

2 (c) A participant in an ~~[the]~~ information sharing and
3 analysis organization established under this section shall assert
4 any exception available under state or federal law, including
5 Section 552.139, in response to a request for public disclosure of
6 information shared through the organization. Section 552.007 does
7 not apply to information described by this subsection.

8 SECTION 3. The heading to Section 2054.068, Government
9 Code, is amended to read as follows:

10 Sec. 2054.068. STATE AGENCY INFORMATION TECHNOLOGY
11 INFRASTRUCTURE: INFORMATION SECURITY RATING; AUDIT; REPORT.

12 SECTION 4. Section 2054.068, Government Code, is amended by
13 amending Subsections (b), (c), and (d) and adding Subsections
14 (c-1), (c-2), (c-3), (c-4), (e-1), (e-2), and (e-3) to read as
15 follows:

16 (b) The department shall collect from each state agency
17 information on the status and condition of the agency's information
18 technology infrastructure, including ~~[information regarding]~~:

19 (1) information on the agency's information security
20 program;

21 (2) an inventory of the agency's servers, mainframes,
22 cloud services, and other information technology equipment;

23 (3) identification information for ~~[of]~~ vendors that
24 operate and manage the agency's information technology
25 infrastructure; ~~[and]~~

26 (4) the results of the information security assessment
27 required by Section 2054.515; and

1 (5) any additional related information requested by
2 the department.

3 (c) A state agency shall provide the information required by
4 Subsection (b) to the department not later than June 1 of each
5 even-numbered year [~~according to a schedule determined by the~~
6 ~~department~~].

7 (c-1) The department shall assign to each state agency that
8 is not an institution of higher education one of the following
9 information security ratings based on the agency's information
10 security risk profile:

11 (1) above average;

12 (2) average; or

13 (3) below average.

14 (c-2) In assigning an information security rating to a state
15 agency under Subsection (c-1), the department shall consider:

16 (1) the information the agency provides under
17 Subsection (b);

18 (2) the agency's comprehensive information security
19 risk position relative to the agency's risk environment; and

20 (3) any additional document or information the
21 department requests from the agency.

22 (c-3) The department:

23 (1) shall develop options and make recommendations for
24 improvements in the information security maturity of any state
25 agency assigned an information security rating of below average
26 under Subsection (c-1); and

27 (2) may assist any state agency in determining whether

1 additional security measures would increase the agency's
2 information security maturity.

3 (c-4) The department may audit the information security and
4 technology of any state agency assigned an information security
5 rating under Subsection (c-1) or contract with a vendor to perform
6 the audit. The department shall make available on request by any
7 person listed in Subsection (d) the results of an audit conducted
8 under this subsection.

9 (d) Not later than November 15 of each even-numbered year,
10 the department shall submit to the governor, chair of the house
11 appropriations committee, chair of the senate finance committee,
12 speaker of the house of representatives, lieutenant governor, and
13 staff of the Legislative Budget Board:

14 (1) a consolidated report of the information submitted
15 by state agencies under Subsection (b); and

16 (2) any department recommendations relevant to and
17 necessary for improving this state's information technology
18 infrastructure and information security.

19 (e-1) The department shall compile a summary of the
20 consolidated report required under Subsection (d) and make the
21 summary available to the public. The summary may not disclose any
22 confidential information.

23 (e-2) The consolidated report required under Subsection (d)
24 and all information a state agency submits to substantiate or
25 otherwise related to the report are confidential and not subject to
26 disclosure under Chapter 552. The state agency or the department
27 may redact or withhold information as confidential under Chapter

1 552 without requesting a decision from the attorney general under
2 Subchapter G, Chapter 552.

3 (e-3) Following its review of the consolidated report, the
4 Legislative Budget Board may direct the department to select for
5 participation in a statewide technology center established under
6 Subchapter L any state agency assigned an information security
7 rating under Subsection (c-1). The department shall notify each
8 selected state agency of the agency's selection as required by
9 Section 2054.385. The department is not required to conduct the
10 cost and requirements analysis under Section 2054.384 for a state
11 agency selected for participation under this subsection. This
12 subsection expires September 1, 2027.

13 SECTION 5. Section 2054.136, Government Code, is amended to
14 read as follows:

15 Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER.

16 (a) Each state agency shall designate an information security
17 officer who:

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

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

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

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

26 (b) An employee designated under Subsection (a) may be
27 designated to serve as a joint information security officer by two

or more state agencies. The department must approve the joint designation.

SECTION 6. The heading to Section 2054.515, Government Code, is amended to read as follows:

Sec. 2054.515. STATE AGENCY INFORMATION SECURITY ASSESSMENT [~~AND REPORT~~].

SECTION 7. Sections 2054.515(a), (c), and (d), Government Code, are amended to read as follows:

(a) At least once every two years, each state agency shall conduct an information security assessment of the agency's[÷

~~[(1)]~~ information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities[÷and

~~[(2) data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by department rule].~~

(c) Each state agency shall complete the information security assessment in consultation with the department or the vendor the department selects and submit the results of the assessment to the department in accordance with Section 2054.068(b) [~~The department by rule shall establish the requirements for the information security assessment and report required by this section~~].

(d) All [~~The report and all~~] documentation related to the information security assessment is [~~and report are~~] confidential and not subject to disclosure under Chapter 552. The state agency or department may redact or withhold the information as

1 confidential under Chapter 552 without requesting a decision from
2 the attorney general under Subchapter G, Chapter 552.

3 SECTION 8. Section 2054.577(c), Government Code, is amended
4 to read as follows:

5 (c) Money in the fund:

6 (1) may be used to improve and modernize state agency
7 information resources, including legacy system projects and
8 cybersecurity projects; ~~and~~

9 (2) may be used to mitigate a security incident at a
10 state agency;

11 (3) may not be used to replace money appropriated to a
12 state agency for the purposes of operating and maintaining state
13 agency information resources or reduce the amount of money
14 appropriated to a state agency for those purposes; and

15 (4) may not be used to pay an entity that commits the
16 crime of electronic data tampering.

17 SECTION 9. Section 2054.1125, Government Code, is
18 transferred to Subchapter R, Chapter 2054, Government Code,
19 redesignated as Section 2054.603, Government Code, and amended to
20 read as follows:

21 Sec. 2054.603 [~~2054.1125~~]. SECURITY INCIDENT [~~BREACH~~]
22 NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) In this
23 section:

24 (1) "Security incident" means:

25 (A) the actual or suspected deliberate and
26 unauthorized access, disclosure, exposure, modification, or
27 destruction of sensitive personal information, confidential

1 information, or other information the disclosure of which is
2 regulated by law through a computer, computer network, or computer
3 system, including:

4 (i) a breach or suspected breach ["Breach]
5 of system security as defined [security" has the meaning assigned]
6 by Section 521.053, Business & Commerce Code; and

7 (ii) the introduction of ransomware, as
8 defined by Section 33.023, Penal Code, into a computer, computer
9 network, or computer system; or

10 (B) a deliberate and unauthorized modification,
11 disruption, destruction, or defacement that makes unavailable or
12 inaccessible:

13 (i) state agency information or information
14 resources; or

15 (ii) a state agency website.

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

18 (b) A state agency or local government that owns, licenses,
19 or maintains computerized data that includes sensitive personal
20 information, confidential information, or information the
21 disclosure of which is regulated by law shall, in the event of a
22 security incident [breach or suspected breach of system security or
23 an unauthorized exposure of that information]:

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

27 (2) not later than 24 ~~[48]~~ hours after the discovery of

1 the security incident [~~breach, suspected breach, or unauthorized~~
2 ~~exposure~~], notify:

3 (A) the department, including the chief
4 information security officer; or

5 (B) if the security incident [~~breach, suspected~~
6 ~~breach, or unauthorized exposure~~] involves election data, the
7 secretary of state; and

8 (3) comply with all department rules relating to
9 security incidents.

10 (c) Not later than the 10th business day after the date of
11 the eradication, closure, and recovery from a security incident
12 [~~breach, suspected breach, or unauthorized exposure~~], a state
13 agency or local government shall notify the department, including
14 the chief information security officer, of the details of the
15 security incident [~~event~~] and include in the notification an
16 analysis of the cause of the security incident [~~event~~].

17 SECTION 10. The following provisions are repealed:

18 (1) Section 2054.068(f), Government Code; and

19 (2) Section 2054.515(b), Government Code, as amended
20 by Chapters 567 (S.B. 475) and 856 (S.B. 800), Acts of the 87th
21 Legislature, Regular Session, 2021.

22 SECTION 11. This Act takes effect September 1, 2023.