2023S0195-1 02/22/23

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 established under this section.

(c)  A participant in an [~~the~~] information sharing and analysis organization established under this section shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of

information shared through the organization. Section 552.007 does

not apply to information described by this subsection.

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

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

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

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

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

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

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

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

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

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

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

(1)  above average;

(2)  average; or

(3)  below average.

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

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

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

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

(c-3)  The department:

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

(2)  may assist any state agency in determining whether additional security measures would increase the agency's information security maturity.

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

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

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

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

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

(e-2)  The consolidated report required under Subsection (d) and all information a state agency submits to substantiate or otherwise related to the report are confidential and not subject to disclosure under Chapter 552. The state agency or the department may redact or withhold information as confidential under Chapter 552 without requesting a decision from the attorney general under Subchapter G, Chapter 552.

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

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

Sec. 2054.136.  DESIGNATED INFORMATION SECURITY OFFICER. (a) Each state agency shall designate an information security officer who:

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

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

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

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

(b)  An employee designated under Subsection (a) may be 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 confidential under Chapter 552 without requesting a decision from the attorney general under Subchapter G, Chapter 552.

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

(c)  Money in the fund:

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

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

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

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

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

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

(1)  "Security incident" means:

(A)  the actual or suspected deliberate and unauthorized access, disclosure, exposure, modification, or destruction of sensitive personal information, confidential information, or other information the disclosure of which is regulated by law through a computer, computer network, or computer system, including:

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

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

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

(i)  state agency information or information resources; or

(ii)  a state agency website.

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

(b)  A state agency or local government 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 security incident [~~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 24 [~~48~~] hours after the discovery of the security incident [~~breach, suspected breach, or unauthorized exposure~~], notify:

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

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

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

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

SECTION 10.  The following provisions are repealed:

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

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

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