BILL ANALYSIS

Senate Research Center

S.B. 1204
By: Paxton
Business & Commerce
3/27/2023
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

H.B. 4018 (87R) created the Joint Oversight Committee on Investment in Information Technology Improvement and Modernization Projects (H.B. 4018 Joint IT Committee) to review investment and funding strategies to modernize state agency information technology infrastructure. In numerous discussions with state agencies, specifically the Department of Information Resources (DIR), over the interim, observations were made about the need to enhance the cybersecurity posture of state agencies ad local governments. The H.B. 4018 Joint IT Committee did not make formal recommendations to the legislature, but these best practices are offered to enhance and improve the cybersecurity posture of the state as a whole. Individual projects at agencies are subject to legislative appropriations and are not included in S.B. 1204.

S.B. 1204 seeks to improve the cybersecurity posture of the state through expanded information sharing, cybersecurity assessments, and security incident reporting.

As proposed, S.B. 1204 amends current law relating to state and local government information technology infrastructure, information security, and data breach and exposure reporting.

RULEMAKING AUTHORITY

Rulemaking authority previously granted to the Department of Information Resources is rescinded in SECTION 7 (Section 2054.515, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends the heading to Section 2054.0594, Government Code, to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.

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

(a) Requires the Department of Information Resources (DIR) to 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 private sector entities in this state to share information regarding cybersecurity threats, best practices, and remediation strategies. Makes a nonsubstantive change.

(a-1) Authorizes DIR to 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) Requires DIR to provide administrative support to each information sharing and analysis organization established under this section. Makes a conforming change.

(c) Makes conforming changes to this subsection.

SECTION 3. Amends the heading to Section 2054.068, Government Code, to read as follows:

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

SECTION 4. Amends Section 2054.068, Government Code, 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), as follows:

(b) Requires DIR to collect from each state agency information on the status and condition of the agency's information technology infrastructure, including, rather than information regarding:

(1)-(3) makes nonsubstantive changes to these subdivisions;

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

(5) creates this subdivision from existing text.

(c) Requires a state agency to provide the information required by Subsection (b) to DIR not later than June 1 of each even-numbered year, rather than according to a schedule determined by DIR.

(c-1) Requires DIR to 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: above average; average; or below average.

(c-2) Requires DIR, in assigning an information security rating to a state agency under Subsection (c-1), to consider the information the agency provides under Subsection (b), the agency's comprehensive information security risk position relative to the agency's risk environment, and any additional document or information DIR requests from the agency.

(c-3) Provides that DIR is required to 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 is authorized to assist any state agency in determining whether additional security measures would increase the agency's information security maturity.

(c-4) Authorizes DIR to 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. Requires DIR to make available on request by any person listed in Subsection (d) the results of an audit conducted under this subsection.

(d) Requires DIR, not later than November 15 of each even-numbered year, to 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 (LBB):

(1) creates this subdivision from existing text; and

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

(e-1) Requires DIR to compile a summary of the consolidated report required under Subsection (d) and make the summary available to the public. Prohibits the summary from disclosing any confidential information.

(e-2) Provides that 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 (Public Information). Authorizes the state agency or DIR to redact or withhold information as confidential

under Chapter 552 without requesting a decision from the attorney general under Subchapter G (Attorney General Decisions), Chapter 552.

(e-3) Authorizes LBB, following its review of the consolidated report, to direct DIR to select for participation in a statewide technology center established under Subchapter L (Statewide Technology Centers) any state agency assigned an information security rating under Subsection (c-1). Requires DIR to notify each selected state agency of the agency's selection as required by Section 2054.385 (Notice of Selection). Provides that DIR is not required to conduct the cost and requirements analysis under Section 2054.384 (Cost and Requirements Analysis) for a state agency selected for participation under this subsection. Provides that this subsection expires September 1, 2027.

SECTION 5. Amends Section 2054.136, Government Code, as follows:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER. (a) Requires each state agency to designate an information security officer who meets certain criteria.

(b) Authorizes an employee designated under Subsection (a) to be designated to serve as a joint information security officer by two or more state agencies. Requires DIR to approve the joint designation.

SECTION 6. Amends the heading to Section 2054.515, Government Code, to read as follows:

Sec. 2054.515. STATE AGENCY INFORMATION SECURITY ASSESSMENT.

SECTION 7. Amends Sections 2054.515(a), (c), and (d), Government Code, as follows:

(a) Requires each state agency, at least once every two years, to conduct an information security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities. Deletes existing text requiring each state agency, at least once every two years, to conduct an information security assessment of the agency's data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by DIR rule. Makes nonsubstantive changes.

(c) Requires each state agency to complete the information security assessment in consultation with DIR or the vendor DIR selects and submit the results of the assessment to DIR in accordance with Section 2054.068(b) (relating to requiring DIR to collect from each state agency information on the status and condition of the agency's information technology infrastructure, including certain information). Deletes existing text requiring DIR by rule to establish the requirements for the information security assessment and report required by this section.

(d) Provides that all documentation, rather than the report and all documentation, related to the information security assessment is confidential and not subject to disclosure under Chapter 552. Makes a conforming change.

SECTION 8. Amends Section 2054.577(c), Government Code, as follows:

(c) Provides that money in the fund:

(1) makes a nonsubstantive change to this subdivision;

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

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

(4) is prohibited from being used to pay an entity that commits the crime of electronic data tampering.

SECTION 9. Transfers Section 2054.1125, Government Code, to Subchapter R, Chapter 2054, Government Code, redesignates it as Section 2054.603, Government Code, and amends it, as follows:

Sec. 2054.603. New heading: SECURITY INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) Defines "security incident" and deletes existing text defining "breach of system security."

(b) Requires 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 is, in the event of a security incident, rather than in the event of a breach or suspected breach of system security or an unauthorized exposure of that information to:

(1) makes a nonsubstantive change to this subdivision;

(2) not later than 24 hours, rather than 48 hours, after the discovery of the security incident, notify:

(A) makes no changes to this paragraph; or

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

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

(c) Requires a state agency or local government, not later than the 10th business day after the date of the eradication, closure, and recovery from a security incident, to notify DIR, including the chief information security officer, of the details of the security incident, rather than event, and include in the notification an analysis of the cause of the security incident.

Makes conforming and nonsubstantive changes.

SECTION 10. Repealers: Section 2054.068(f) (relating to providing that the consolidated report submitted is public information and is required to be released or made available to the public on request, with an exception), Government Code, and Section 2054.515(b) (relating to requiring the agency to report the results of the assessment), 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. Effective date: September 1, 2023.