

BILL ANALYSIS

S.B. 1779
By: Paxton
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

The 85th Texas Legislature established the Senate Select Committee on Cybersecurity to study and issue a report on the state's cybersecurity policy. Interim hearings held by the committee identified several areas where the state could benefit from improvements and updates to state law to better protect state agency data and ensure that key services are delivered adequately, including by strengthening state oversight of cybersecurity practices. S.B. 1779 seeks to implement those improvements and make the necessary updates to state law.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Department of Information Resources in SECTIONS 2 and 20 of this bill.

ANALYSIS

S.B. 1779 amends the Government Code to revise, add, transfer, and redesignate certain provisions regarding security for state agency information and information technologies. The bill authorizes the Department of Information Resources (DIR) to adopt rules as necessary to implement its responsibilities under the bill's provisions.

S.B. 1779 authorizes DIR to require each applicable state agency to report the following to DIR:

- each agency's use of information security and cybersecurity technologies;
- the effect of those technologies on the duties and functions of the agency;
- the costs incurred by the agency in the acquisition and use of those technologies;
- the procedures followed in obtaining those technologies; and
- other information relating to information security and cybersecurity management that in the judgment of DIR should be reported.

S.B. 1779 authorizes DIR, at the request of an applicable state agency, to provide technical and managerial assistance relating to information security and cybersecurity management and technologies. The bill authorizes DIR to report to the governor and the presiding officer of each house of the legislature any factors that in the opinion of DIR are outside the duties of DIR but that inhibit or promote effective communication about the use of information security and cybersecurity in state government.

S.B. 1779 revises the required contents of the biennial DIR cybersecurity report by:

- removing the requirement for the report to include an evaluation of the following:
 - the costs and benefits of cybersecurity insurance; and
 - tertiary disaster recovery options; and
- requiring the report to include an evaluation of a program that provides an information security officer to assist small applicable state agencies and local governments that are unable to justify hiring a full-time information security officer.

S.B. 1779 replaces the requirement for DIR to establish an information sharing and analysis center with a requirement for DIR to establish an information sharing and analysis organization to provide a forum for applicable 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. The bill requires DIR to provide administrative support to the organization. The bill requires a participant in the organization to assert any exception available under state or federal law in response to a request for public disclosure of information shared through the organization and prohibits a participant from voluntarily making certain information not required to be disclosed available to the public.

S.B. 1779 authorizes two or more applicable state agencies, on approval from DIR, to jointly designate an information security officer to serve as the information security officer for each agency. The bill authorizes DIR to provide information security training for appointed board members, agency heads, and executive management of state agencies that is consistent with the cybersecurity awareness training provided by each state agency to agency employees who handle sensitive information.

S.B. 1779 removes the state cybersecurity coordinator from the entities that an applicable 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 must notify not later than 48 hours after the discovery of a breach or suspected breach of system security or an unauthorized exposure of that information. The bill requires an agency, not later than the 10th business day after the date of the eradication, closure, and recovery from the breach, suspected breach, or unauthorized exposure, to notify DIR, including the chief information security officer, of the details of the event.

S.B. 1779 transfers from an applicable state agency's information resources manager to the agency's information security officer the responsibility to prepare or have prepared a biennial report assessing the vulnerability of certain agency technology. The bill includes among the entities to which an electronic copy of the vulnerability report is required to be provided on its completion the agency's designated information resource manager. The bill specifies that an agency's information resources officer is the individual responsible for preparing a summary of the agency's vulnerability report that is separate from the executive summary of the report.

S.B. 1779 requires the written acknowledgment included in an applicable state agency's information security plan of the fact that the agency head, chief financial officer, and each applicable executive manager have been made aware of the risks revealed during the preparation of the security plan to be in the form of a written document that is signed by each such person and that states that each such person has been made aware of those risks.

S.B. 1779 removes the governor, the lieutenant governor, and the speaker of the house of representatives as recipients of an applicable state agency's report of the results of its periodic information security assessment but authorizes such an officer to obtain the report upon request to DIR. The bill replaces the authorization for DIR to establish by rule requirements for such an assessment and report with a requirement for DIR to do so.

S.B. 1779 repeals provisions of the Information Resources Management Act regarding data security procedures for online and mobile applications for public institutions of higher education and makes applicable to those institutions provisions regarding a certain data security plan for online and mobile applications that are applicable to each applicable state agency implementing a website or mobile application that processes any sensitive personally identifiable information or confidential information.

S.B. 1779 repeals the requirement for DIR to provide mandatory guidelines to applicable state agencies regarding the continuing education requirements for cybersecurity training that must be completed by all information resources employees of the agencies.

S.B. 1779 requires DIR to develop recommendations for cybersecurity and information resources and technology security training for personnel of an applicable state agency and post those recommendations on the DIR website. The bill clarifies that the provisions of an agreement between DIR and a national organization to support DIR efforts in implementing the components of the plan to address cybersecurity risks and incidents in Texas regarding training and related exercises for state agencies apply with respect to the state agency personnel.

S.B. 1779 requires the information security officer of each applicable state agency to submit an information security report for the agency not later than October 15 of each even-numbered year that includes the following:

- the agency's vulnerability report;
- the agency's information security plan;
- the agency's information security assessment;
- the agency's data security plan for online and mobile applications; and
- the recommendations for cybersecurity and information resources and technology security training developed by DIR.

S.B. 1779 exempts the Teacher Retirement System of Texas (TRS) from the application of the bill's provisions relating to information security but requires TRS to comply with the cybersecurity and information security standards established by DIR under those bill provisions. The bill requires the Employees Retirement System of Texas to comply with those standards.

S.B. 1779 requires DIR, not later than August 31, 2020, to adopt rules necessary to implement the bill's changes in law. The bill provides that a rule adopted by DIR under the Information Resources Management Act related to information security and cybersecurity continues in effect under the bill's provisions.

S.B. 1779 repeals the following Government Code provisions:

- Section 2054.076(b-1)
- Section 2054.514
- Section 2054.517
- the heading to Subchapter N-1, Chapter 2054

EFFECTIVE DATE

September 1, 2019.