# BILL ANALYSIS

S.B. 64
By: Nelson
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, bolstering the cybersecurity workforce, assisting local government recovering from cybersecurity events, and improving oversight of the state's electric grid. S.B. 64 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 this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

## ANALYSIS

S.B. 64 amends the Education Code to require the Texas Higher Education Coordinating Board, in collaboration with the Department of Information Resources (DIR), to identify and develop strategies to incentivize public institutions of higher education to develop degree programs in cybersecurity. The bill requires the coordinating board, not later than September 1, 2020, to submit a written report detailing those strategies to the lieutenant governor, the speaker of the house of representatives, the presiding officer of each legislative standing committee with primary jurisdiction over higher education, and each governing board of a public institution of higher education. The bill requires the coordinating board to consult with those institutions as necessary to carry out these duties. These provisions expire September 1, 2021.

S.B. 64 amends the Government Code to include a cybersecurity event among the events the occurrence or imminent threat of which constitutes a disaster for purposes of the Texas Disaster Act of 1975.

S.B. 64 requires the Employees Retirement System of Texas and the Teacher Retirement System of Texas to comply with cybersecurity and information security standards established by DIR under the Information Resources Management Act. The bill expands the circumstances under which that act applies to a public junior college or a public junior college district to include compliance with such information security standards and to participate in shared technology services.

S.B. 64 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 state agencies and local governments that are unable to justify hiring a full-time information security officer.

S.B. 64 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 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 and 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. The bill exempts such information from provisions of state public information law governing the voluntary disclosure of certain information when disclosure is not required.

S.B. 64 revises the required contents of the biennial consolidated DIR report on the status and condition of each state agency's information technology infrastructure by removing the requirement for that report to include, for an agency found to be at higher security and operational risks, a detailed analysis and estimate of the costs to implement certain requirements for the agency to address risks and vulnerabilities and agency efforts regarding those risks and vulnerabilities. The bill requires that report to include instead for such an agency a detailed analysis of agency efforts to address those agency risks and related vulnerabilities.

S.B. 64 requires DIR, not later than October 1 of each even-numbered year, to submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects and projects to modernize or replace legacy systems. The bill requires a state agency to assert any exception available under state or federal law in response to a request for public disclosure of information contained in or written, produced, collected, assembled, or maintained in connection with the report and exempts such information from the application of the provisions of state public information law governing the voluntary disclosure of certain information when disclosure is not required. The bill requires each state agency to coordinate with DIR to implement these provisions.

S.B. 64 transfers from a 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 report is required to be provided on its completion the agency's designated information resources manager.

S.B. 64 removes the state cybersecurity coordinator from the entities that a 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, including an analysis of the cause of the event.

S.B. 64 requires the written acknowledgment included in a 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. The bill authorizes DIR to provide by agreement network security to a public junior college.

S.B. 64 repeals provisions of the Information Resources Management Act relating to bids or proposals for interagency contracts for the receipt of information resources technologies. The bill repeals provisions of that 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 state agency implementing a website or mobile application that processes any sensitive personal or personally identifiable information or confidential information.

S.B. 64 amends the Occupations Code to establish that the review and analysis of computer-based data by an investigations company for the purpose of preparing for or responding to a cybersecurity event does not constitute an investigation by the company and does not require licensing under the Private Security Act.

S.B. 64 amends the Utilities Code to require the Public Utility Commission of Texas (PUC) to establish a program to monitor cybersecurity efforts among the following types of utilities in Texas:

- electric cooperatives;
- electric utilities;
- municipally owned electric utilities;
- retail electric providers; and
- transmission and distribution utilities.

The bill sets out the required components of the program and authorizes the PUC to collaborate with the state cybersecurity coordinator and the cybersecurity council in its implementation.

S.B. 64 requires an independent organization certified by the PUC to perform certain functions related to the market structure of the electric utility industry under the Public Utility Regulatory Act to do the following:

- conduct internal cybersecurity risk assessment, vulnerability testing, and employee training to the extent the organization is not otherwise required to do so under applicable state and federal cybersecurity and information security laws; and
- submit a report annually to the PUC on the organization's compliance with such applicable laws.

The bill makes information submitted in that annual report confidential and exempt from disclosure under state public information law.

S.B. 64 repeals the following provisions of the Government Code:

- Section 2054.119
- Section 2054.517

**EFFECTIVE DATE**

September 1, 2019.