BILL ANALYSIS

S.B. 35
By: Zaffirini
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

Interested observers point out that Texas increasingly relies on technology to manage the personal information of more than 26 million citizens and to run its infrastructure efficiently. Consequently, these observers agree that establishing a robust cybersecurity system must be a priority for state agencies. Cybersecurity experts report that one of the main causes of a cyber-attack that compromise the personal information of a private company's customers is the lack of direct communication between the company's cybersecurity officers and the company's leadership, and the observers contend that a state agency is exposed to the same cyber-attack risk as a private company. These observers also note that many state agencies designate a chief information security officer to prepare and submit a biennial cybersecurity plan to the Department of Information Resources but contend that the agency's leadership is not required to confer with its security officer regarding the plan. In order to improve communication and accountability regarding cybersecurity plans, S.B. 35 seeks to require the acknowledgement by state agency management of the risks identified in state agency information security plans.

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. 35 amends the Government Code to require each state agency to include in the agency's information security plan a written acknowledgment that the executive director or other head of the state agency, the chief financial officer, and each executive manager as designated by the state agency have been made aware of the risks revealed during the preparation of the agency's information security plan.

EFFECTIVE DATE

September 1, 2015.