BILL ANALYSIS

S.B. 1597
By: Zaffirini
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

Although cyber-attacks generally are not widely publicized, interested parties note that cyber-attacks occur routinely, potentially costing millions of dollars, damaging critical infrastructure, and consequently undermining confidence in information systems, including those of governmental entities in Texas. Interested parties further note that, despite the best efforts of the Department of Information Resources, preventing human error remains a challenge, the need to respond proactively persists, and ensuring that each agency has adequate policies and procedures in place that are followed by all employees can help mitigate some of these threats. Although current law requires the information resources manager of a state agency to prepare or have prepared a report on the vulnerabilities of the agency's information security, the parties suggest that these vulnerabilities could be further addressed by directing each state agency to develop an information security plan to secure the agency's information. S.B. 1597 seeks to establish this requirement.

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. 1597 amends the Government Code to require each state agency to develop and periodically update an information security plan for protecting the security of the agency's information. The bill requires a state agency, in developing such a plan, to do the following:

- consider any vulnerability report prepared for the agency by the agency's information resources manager or at the manager's direction;
- incorporate the network security services provided by the Department of Information Resources (DIR) to the agency;
- identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;
- identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;
- include the best practices for information security developed by DIR or a written explanation of why the best practices are not sufficient for the agency's security; and
- omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online system.

The bill requires each state agency to develop and submit the information security plan required under the bill's provisions not later than October 15, 2014, and to submit a copy of the agency's information security plan to DIR not later than October 15 of each even-numbered year. The bill establishes that each state agency's information security plan is confidential and exempt from disclosure under state public information law.

EFFECTIVE DATE

September 1, 2013.