# BILL ANALYSIS

Senate Research Center
83R17758 YDB-D

C.S.S.B. 1597
By: Zaffirini
Government Organization
3/26/2013
Committee Report (Substituted)

## AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Although not widely publicized, cyber attacks occur routinely. Cybercrime and intrusions cost millions of dollars, damage critical infrastructure, and undermine Texans' confidence in state information systems. Despite the best efforts of the Department of Information Resources, human error remains a challenge, and the need to respond proactively persists.

Ensuring that each agency has adequate policies and procedures in place that are followed by all employees can help mitigate some of these threats. Section 2054.077 (Vulnerability Reports), Government Code, requires the information resources manager of a state agency to prepare a report on the vulnerabilities of the agency's information security.

This bill complements current law by directing each state agency to develop an information security plan to protect the security of the agency's information, thereby addressing vulnerabilities and improving the security of the agency's information systems.

C.S.S.B. 1597 amends current law relating to the development of state agency information security plans.

## RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

## SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter F, Chapter 2054, Government Code, by adding Section 2054.133, as follows:

> Sec. 2054.133. INFORMATION SECURITY PLAN. (a) Requires each state agency to develop, and periodically update, an information security plan for protecting the security of the agency's information.
>
> (b) Requires the state agency, in developing the plan, to:
>
> (1) consider any vulnerability report prepared under Section 2054.077 (Vulnerability Reports) for the agency;
>
> (2) incorporate the network security services provided by the Department of Information Resources (DIR) to the agency under Chapter 2059 (Texas Computer Network Security System);
>
> (3) identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;
>
> (4) identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction; and

(5) 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

(6) omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

(c) Requires each state agency, not later than October 15 of each even-numbered year, to submit a copy of the agency's information security plan to DIR.

(d) Provides each state agency's information security plan is confidential and exempt from disclosure under Chapter 552 (Public Information).

SECTION 2. Requires each state agency, not later than October 15, 2014, to develop and submit the information security plan as required by Section 2054.133, Government Code, as added by this Act.

SECTION 3. Effective date: September 1, 2013.