

## **BILL ANALYSIS**

Senate Research Center

S.B. 34  
By: Zaffirini  
Business & Commerce  
5/28/2015  
Enrolled

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

The State of Texas increasingly relies on technology to manage the personal information of more than 26 million citizens and to run its infrastructure efficiently. Accordingly, the establishment of a robust cyber-protection system must be a priority for the State. Cybersecurity experts indicate that one of the main causes of cyber-attacks that compromise the personal information of millions of private companies' customers is the lack of a direct communication channel between the companies' cybersecurity officers and the companies' leadership. The State of Texas is exposed to the same risk of suffering cyber-attacks as the business community. The Department of Information Resources (DIR) manages cybersecurity information from state agencies, but lacks a formal mechanism to communicate its analysis of this information and make recommendations to legislators and policymakers.

S.B. 34 seeks to provide for a biennial report that would serve as that formal channel for DIR to communicate findings and suggestions to state leaders to facilitate the formulation of policies that increase the security of the state's and our citizens' information.

S.B. 34 amends current law relating to a report concerning information security for this state's information resources.

### **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 Section 2054.133, Government Code, by adding Subsection (f), as follows:

(f) Requires the Texas Department of Information Resources (DIR) to submit a written report to the governor, the lieutenant governor, and the legislature evaluating information security for this state's information resources not later than January 13 of each odd-numbered year. Requires DIR, in preparing the report, to consider the information security plans submitted by state agencies under this section, any vulnerability reports submitted under Section 2054.077 (Vulnerability Reports), and other available information regarding the security of this state's information resources. Requires DIR to omit from any written copies of the report information that could expose specific vulnerabilities in the security of this state's information resources.

SECTION 2. Effective date: September 1, 2015.