# BILL ANALYSIS

Senate Research Center
85R1107 AAF-D

S.B. 56
By: Zaffirini
Business & Commerce
2/8/2017
As Filed

## 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 state agencies. 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 direct communication between the companies' cybersecurity officers and the companies' leadership. State agencies are exposed to the same risk of suffering cyber-attacks as private companies. Most agencies designate their Chief Information Security Officer (CISO) to prepare and submit a biennial cybersecurity plan to the Department of Information Resources (DIR), but the agency's leadership is not required to confer with its CISO regarding these cybersecurity plans. S.B. 56 would require agency leadership to sign the agencies' biennial cybersecurity plans to improve communication and accountability regarding cybersecurity programs.

As proposed, S.B. 56 amends current law relating to the acknowledgment by management of risks identified in 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 Section 2054.133, Government Code, by adding Subsection (e) to require that each state agency include in the agency's information security plan a written acknowledgement that certain named individuals designated by the state agency have been made aware of the risks revealed during the preparation of the agency's information security plan.

SECTION 2. Effective date: September 1, 2017.