BILL ANALYSIS

Senate Research Center
83R6585 MTB-D

S.B. 1134
By: Ellis
Government Organization
3/22/2013
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

S.B. 1134 seeks to update and codify the duties of the Department of Information Resources (DIR) with regard to cybersecurity.

Current law allows DIR to establish and administer a clearinghouse for information relating to all aspects of protecting the security of state agency information. DIR's authority on cybersecurity comes from rule (1 TAC 202).

In the recent past, a number of state agencies have experienced data breaches that affected millions of Texans. One of these breaches involved highly confidential personal information that was publically accessible over the Internet for over a year, while others were as simple as an employee mistakenly attaching a document with confidential information to an email. These and a number of other data breaches were due to human error.

It is clear that human error plays a large role in the security breaches that various state agencies have experienced in the last several years. At the same time, the threat posed by hackers and other malicious actors cannot be overlooked. Technology is advancing so fast that it can be difficult for information technology departments to keep up with the changes, increasing the risk of attack.

S.B. 1134 will allows DIR, within existing resources, the ability to expand its leadership role in developing strategies, training, awareness and best practices in cybersecurity, and a framework for securing cyber infrastructure by state agencies.

As proposed, S.B. 1134 amends current law relating to the duties of the Department of Information Resources regarding cybersecurity.

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 2054.059, Government Code, as follows:

> Sec. 2054.059. New heading: CYBERSECURITY. Requires the Department of Information Resources (DIR), from available funds, to:
>
> > (1) establish and administer a clearinghouse for information relating to all aspects of protecting the cybersecurity, rather than security, of state agency information;
> >
> > (2) develop strategies and a framework for:
> >
> > > (A) the securing of cyberinfrastructure by state agencies, including critical infrastructure; and
> > >
> > > (B) cybersecurity risk assessment and mitigation planning;

(3) develop and provide training to state agencies on cybersecurity measures and awareness;

(4) provide assistance to state agencies on request regarding the strategies and framework developed under Subdivision (2); and

(5) promote public awareness of cybersecurity issues.

Makes nonsubstantive changes.

SECTION 2. Effective date: September 1, 2013.