BILL ANALYSIS

Senate Research Center
84R11310 DDT-D

S.B. 1878
By: Zaffirini
Business & Commerce
4/7/2015
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The purpose of this legislation is to direct the Department of Information Resources (DIR) to conduct a feasibility study regarding the adoption of an additional layer of sensitive data control and security.

Two-step authentication, also known as multi-factor authentication, is a process in which a user must pass more than one form of access control to a enter a network or database. Most commonly, this process entails entering a username and password coupled with a subsequent text message, or sometimes an email to a separate account, containing a unique numeric code. In this way, even if an attacker managed to retrieve a user's username and password, the attacker would still not be granted access because they require the code sent to the user's personal phone or separate email account. This form of access control has been adopted by many businesses and email providers because it creates an effective additional layer of control and security.

At the state level, large strides have been made to secure personal and private information from external threats, but less concrete action has been done on the internal access side beyond simple password protection and broad user restrictions, which places citizens' information at undue risk. The implementation of two-step authentication system would enhance greatly the security of sensitive information.

The success of two-step authentication, however, heavily relies on a comprehensive Identity and Access Management (IAM) program. IAM programs create user profiles, which can be changed as access requirements increase or decrease. It also is a security mechanism that prevents users from accessing information or computers that are unauthorized for their use.

S.B. 1878 builds upon the findings of the Senate Committee on Government Organization and the House Committee on Technology and directs DIR to conduct a thorough study establishing the goals and recommendations to the state regarding the statewide adoption of IAMs and two-step authentication systems. As a result of S.B. 1878, the state establishes a blueprint to ensure that sensitive information of Texans is protected to the fullest extent.

As proposed, S.B. 1878 relates to a study on the feasibility of implementing more secure access requirements for electronically stored information held by the state.

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. STUDY OF IDENTIFICATION AND ACCESS MANAGEMENT. Requires the Department of Information Resources (DIR) to conduct a study to determine the feasibility of implementing new identification and access requirements for accessing certain information that is electronically stored by the state, including personal identifying information and sensitive personal information, as those terms are defined by Section 521.002 (Definitions), Business & Commerce Code.

SECTION 2. COLLABORATION WITH OTHER AGENCIES. Requires DIR, in conducting the study, to collaborate with other agencies to consider the needs or concerns specific to those agencies.

SECTION 3. SCOPE OF STUDY. Requires the study to:

(1) examine the relative costs and benefits of various forms of identification and access management, including multifactor authentication;

(2) evaluate various data loss and recovery systems or programs;

(3) evaluate various security information and event management systems or programs; and

(4) develop a strategy by which DIR may most effectively negotiate for the use of the preferred systems or programs across agencies at the lowest cost to the state.

SECTION 4. REPORT AND RECOMMENDATIONS. (a) Requires DIR to issue a written report to the governor, the lieutenant governor, and the speaker of the house of representatives that includes DIR's evaluation of the available systems and programs and provides recommendations regarding DIR action or legislation that will secure sensitive information held by the state and allow for the best response in the event any information is compromised.

(b) Requires the report to be issued not later than November 30, 2016.

SECTION 5. EXPIRATION. Provides that this Act expires December 1, 2016.

SECTION 6. EFFECTIVE DATE. Effective date: September 1, 2015.