BILL ANALYSIS

Senate Research Center
85R12695 YDB-D

S.B. 1910
By: Zaffirini
Business & Commerce
4/4/2017
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Technological advancements have increased the likelihood of cybersecurity attacks. The private sector is adapting swiftly to this new reality. Best practices in the private sector include independent review of an entity's cyber-security plan, separation between the chief information security officer (CISO) and the information technology departments, and creating data security plans before beta testing mobile applications that handle private information. These practices have not been adopted in the public sector, which make state agencies more prone to cybersecurity risks.

S.B. 1910 requires the Department of Information Resources (DIR) to select a portion of the cybersecurity plans to audit in accordance with DIR rules. This independent review would enhance the accuracy and reliability of state agencies' cybersecurity plans.

What's more, S.B. 1910 requires that agencies with CISO positions have the CISO work independently from the IT division in terms of the organizational structure and budget. This change would result in better allocation of resources for cybersecurity by creating a direct line of communication between the CISO and higher command officers such as the chief financial officer, chief risk officer, or chief of staff.

Lastly, S.B. 1910 requires each state agency to submit a data security plan prior to beta testing an Internet website or mobile app that processes any personally identifiable or confidential information. This requirement would enhance the security of Texans' personal information contained in state mobile apps.

As proposed, S.B. 1910 amends current law relating to state agency information security plans, information technology employees, and online and mobile applications.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Department of Information Resources in SECTION 4 of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Section 2054.133(c), Government Code, to require the Department of Information Resources (DIR) to select a portion of the submitted information security plans to be audited by DIR in accordance with DIR rules.

SECTION 2. Amends Subchapter F, Chapter 2054, Government Code, by adding Section 2054.136, as follows:

> Sec. 2054.136. INDEPENDENT CHIEF INFORMATION SECURITY OFFICER. Requires each state agency in the executive branch of state government that has on staff a chief information security officer to ensure that within the agency's organizational structure the officer is independent from and not subordinate to the agency's information technology operations.

SECTION 3. Amends Subchapter N-1, Chapter 2054, Government Code, by adding Section 2054.516, as follows:

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Requires each state agency implementing an Internet website or mobile application that processes any personally identifiable or confidential information to submit a data security plan to DIR before beta testing the website or application, and before deploying the website or application, subject the website or application to a vulnerability and penetration test conducted by an independent third party, and address any identified vulnerability.

(b) Requires that the data security plan required under Subsection (a)(1) include certain information.

(c) Requires DIR to review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after DIR reviews the plan.

SECTION 4. Requires the DIR, as soon as practicable after the effect date of this Act, to adopt rules necessary to implement Section 2054.133(c), Government Code, as amended by this Act.

SECTION 5. Effective date: September 1, 2017.