BILL ANALYSIS

Senate Research Center

S.B. 1910
By: Zaffirini
Business & Commerce
7/7/2017
Enrolled

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 cybersecurity 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 Texas 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. (Original Author's / Sponsor's Statement of Intent)

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 Texas Department of Information Resources in SECTION 6 of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter C, Chapter 2054, Government Code, by adding Sections 2054.0591 and 2054.0592, as follows:

> Sec. 2054.0591. CYBERSECURITY REPORT. (a) Requires the Texas Department of Information Resources (DIR), not later than November 15 of each even-numbered year, to submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. Requires that the report include certain information.
>
> (b) Authorizes DIR or a recipient of a report under this section to redact or withhold information confidential under Chapter 552 (Public Information), including Section 552.139 (Exception: Confidentiality of Government

Information Related to Security or Infrastructure Issues for Computers), or other state or federal law that is contained in the report in response to a request under Chapter 552 without the necessity of requesting a decision from the Texas attorney general under Subchapter G (Attorney General Decisions), Chapter 552.

Sec. 2054.0592. CYBERSECURITY EMERGENCY FUNDING. Authorizes DIR, if a cybersecurity event creates a need for emergency funding, to request that the governor or Legislative Budget Board (LBB) make a proposal under Chapter 317 (State Budget Execution) to provide funding to manage the operational and financial impacts from the cybersecurity event.

SECTION 2. Amends Subchapter F, Chapter 2054, Government Code, by adding Section 2054.1184, as follows:

Sec. 2054.1184. ASSESSMENT OF MAJOR INFORMATION RESOURCES PROJECT. (a) Requires a state agency proposing to spend appropriated funds for a major information resources project to first conduct an execution capability assessment to determine the agency's capability for implementing the project, reduce the agency's financial risk in implementing the project, and increase the probability of the agency's successful implementation of the project.

(b) Requires a state agency to submit to DIR, the quality assurance team established under Section 2054.158 (Quality Assurance Team; Duties), and LBB a detailed report that identifies the agency's organizational strengths and any weaknesses that will be addressed before the agency initially spends appropriated funds for a major information resources project.

(c) Authorizes a state agency to contract with an independent third party to conduct the assessment under Subsection (a) and prepare the report described by Subsection (b).

SECTION 3. Amends Section 2054.133(c), Government Code, to authorize DIR, subject to available resources, to select a portion of the submitted information security plans to be assessed by DIR in accordance with DIR rules.

SECTION 4. Amends Subchapter F, Chapter 2054, Government Code, by adding Section 2054.136, as follows:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER. Requires each state agency to designate an information security officer with certain duties and training.

SECTION 5. Amends Subchapter N-1, Chapter 2054, Government Code, by adding Sections 2054.516 and 2054.517, 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 sensitive personally identifiable or confidential information, other than an institution of higher education (IHE) subject to Section 2054.517, to submit a biennial data security plan to DIR not later than October 15 of each even-numbered year, to establish beta testing for websites or applications, and subject the website or application to a vulnerability and penetration test and address any identified vulnerability.

(b) 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.

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Requires each IHE, as defined by Section 61.003 (Definitions), Education Code, to adopt and

implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Requires the developer of the website or application for the IHE, before deploying an Internet website or mobile application that processes confidential information for an IHE, to submit to the IHE's information security officer the information required under policies adopted by the IHE to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. Requires that the IHE's policies, at a minimum, require the developer to submit information describing the architecture of the website or application, the authentication mechanism for the website or application, and the administrator-level access to data included in the website or application.

(c) Requires an IHE, before deploying an Internet website or mobile application described by Subsection (b), to subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Requires each IHE to submit to DIR the policies adopted as required by Subsection (b). Requires DIR to review the policies and make recommendations for appropriate changes.

SECTION 6. Requires 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 7. Effective date: September 1, 2017.