SUBJECT: Creating certain information security requirements for state agencies

COMMITTEE: State Affairs — favorable, without amendment

VOTE: 13 ayes — Cook, Giddings, Craddick, Farrar, Geren, Guillen, K. King, Kuempel, Meyer, Oliveira, Paddie, E. Rodriguez, Smithee

SENATE VOTE: On final passage, May 4 — 31-0, on Local and Uncontested Calendar

WITNESSES: No public hearing

BACKGROUND: Government Code, sec. 2054.133 requires each state agency to develop an information security plan for protecting the agency's information from unauthorized access, disclosure, destruction, and other security threats. By October 15 of each even-numbered year, each agency is required to submit a copy of its information security plan to the Department of Information Resources.

As technological advancements have increased the likelihood of cybersecurity attacks, the private sector has adopted certain best practices to address the issue. Observers have noted that state agencies will continue to be prone to cybersecurity risks if they do not take measures to adopt similar practices to enhance the security of agency information, including personally identifiable or confidential information.

DIGEST: SB 1910 would amend current law relating to information security plans, information technology employees, and online and mobile applications.

Audit of information security plans. The Department of Information Resources (DIR) would be required to select a portion of submitted state agency security plans to audit in accordance with department rules and subject to available resources. DIR would adopt rules necessary to implement this requirement as soon as practicable after September 1, 2017.

Independent information security officer. Each agency in the executive

branch of state government that had a chief information security officer or an information security officer would have to ensure that within the agency's organizational structure, the officer was independent from and not subordinate to the agency's information technology operations.

Data security plan for online and mobile applications. Each state agency with a website or mobile application that processes personally identifiable or confidential information would have to submit a data security plan to DIR before beta testing that included relevant security information defined in the bill. DIR would review each plan and make any recommendations to the agency as soon as practicable after the department reviewed the plan.

An agency also would be required to subject such a website or application to a vulnerability and penetration test conducted by a third party and address any vulnerability identified prior to deployment.

The bill would take effect September 1, 2017.

NOTES:

According to the Legislative Budget Board's fiscal note, a cost resulting from the bill is expected but could not be determined. DIR estimates an annual negative impact of $900,000 to the Clearing Fund to perform audits for security plans. Other costs to agencies could result from third-party vulnerability and penetration testing of online and mobile applications.