SUBJECT: Requiring cybersecurity training for certain employees and contractors

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 11 ayes — Phelan, Deshotel, Guerra, Harless, Holland, Hunter, P. King, Parker, Raymond, E. Rodriguez, Springer

0 nays

2 absent — Hernandez, Smithee

WITNESSES: For — (*Registered, but did not testify*: Russell Mullins, Alterity Solutions, Inc.; Jim Keffer, City of Del Rio; James Dickey, Republican Party of Texas; Justin Yancy, Texas Business Leadership Council; Nora Belcher, Texas e-Health Alliance; Deborah Giles, Texas Technology Consortium; Joe Buser, Traveling Coaches, Inc.; Russell Hayter)

Against — None

On — (*Registered, but did not testify*: Troy Alexander, Texas Medical Association)

BACKGROUND: Government Code sec. 2054.518 requires the Department of Information Resources (DIR) to develop a plan to address cybersecurity risks and incidents. To support the plan's implementation, DIR may enter into an agreement with a national organization to provide for certain items as listed in statute.

In selecting a national organization, DIR must consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

It has been noted that the integration of information technology into the duties of many state and local government employees and contractors has created points of vulnerability for government data systems that hold sensitive information. Some have suggested that increased training and

development of best practices could minimize Texas' cybersecurity risk.

DIGEST:

CSHB 3834 would require the Department of Information Resources (DIR), in consultation with the state cybersecurity council and industry stakeholders, to annually certify at least 20 cybersecurity training programs for state and local government employees and to update standards for maintenance of certification by the training programs.

To be certified, a training program would have to include activities, case studies, hypothetical situations, and other methods that focused on forming information security habits and procedures that protected information resources and taught best practices for detecting, assessing, reporting, and addressing threats.

DIR could contract with an independent third party to certify the training programs and would have to annually publish on its website the list of certified programs.

The bill would require a state or local government employee that used a computer for at least 25 percent of the employee's duties to complete a cybersecurity training program at least once a year. A local government or state agency could select the most appropriate training program for its employees and would have to verify program completion and require periodic audits to ensure compliance.

CSHB 3834 would require any contractor who had access to a state computer system or database to complete a cybersecurity training program during the term of the contract and any renewal period. The required completion of a cybersecurity training program would be included in the terms of an awarded contract. A contractor would have to verify program completion to the contracting state agency, and the agency's contract manager would report the completion to DIR and conduct periodic audits to ensure compliance.

Under the bill, DIR no longer would have to consider a national organization's previous experience in conducting cybersecurity training

and exercises for state entities before entering into an agreement for support in implementing a cybersecurity risks and incidents plan under Government Code sec. 2054.518. The agreement no longer would have to include provisions for:

- providing fee reimbursement for appropriate industry-recognized certification exams;
- developing and maintaining a cybersecurity risks and incidents curriculum; or
- delivering to certain state agency personnel routine training related to protecting and maintaining IT systems, implementing best practices, and mitigating cybersecurity risks and incidents.

The bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2019, and would apply to a contract entered into or renewed on or after the effective date.