SUBJECT: Addressing state, local compliance with required cybersecurity training

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 12 ayes — Paddie, Hernandez, Deshotel, Harless, Howard, Hunter, P. King, Lucio, Metcalf, Raymond, Shaheen, Slawson

0 nays

1 absent — Smithee

WITNESSES: For — (*Registered, but did not testify*: Blaire Parker, San Antonio Water System (SAWS); Russell Schaffner, Tarrant County; Mark Terry, TEPSA, Frank Holman; Thomas Parkinson; Ruth York)

Against — (*Registered, but did not testify*: Daniel Collins, County of El Paso, Texas; Ender Reed, Harris County Commissioners Court; Julie Wheeler, Travis County Commissioners Court)

On — (*Registered, but did not testify*: Nancy Rainosek, Department of Information Resources)

BACKGROUND: Government Code sec. 2054.519 requires the Department of Information Resources (DIR) annually to certify for state and local government employees cybersecurity training programs that meet certain criteria. Under sec. 2054.519(f), a local government that employs a dedicated information resources cybersecurity officer may offer its employees a cybersecurity training program that satisfies the criteria used by DIR to certify its training programs.

Sec. 2054.5191(a) requires state agency employees who use a computer to complete at least 25 percent of the employee's required duties and each elected or appointed officer of a state agency to complete a certified cybersecurity training program at least once a year.

Sec. 2054.5191(a-1) requires local government employees who have

access to a computer system or database and local elected officials to complete a certified cybersecurity training program at least once a year.

Sec. 2056.002 requires a state agency biennially to make a strategic plan for its operations that includes elements determined by the Legislative Budget Board and the Office of the Governor.

DIGEST:

CSHB 1118 would expand the required cybersecurity training under Government Code sec. 2054.5191(a-1) to include appointed officials of a local government. The bill would specify that the local government employees and elected and appointed officials who would be required to complete the cybersecurity training program were those who had access to a local government computer system or database and used a computer to perform at least 25 percent of required duties.

Under the bill, the annual cybersecurity training requirement for state agency and local government employees and officials would not apply to employees who had been granted:

- military leave;
- leave under the federal Family and Medical Leave Act of 1993; or
- leave covered by workers' compensation benefits or any other type of extended leave or authorization to work from an alternative work site if the employee no longer had access to the state agency's or local government's database and systems.

CSHB 1118 would repeal a provision that allows a local government that employs a dedicated information resources cybersecurity officer to offer its employees a cybersecurity training program.

The Department of Information Resources (DIR) would have to develop a form for state agencies and local governments to use to verify completion of cybersecurity training program requirements. The form would have to allow an entity to indicate the percentage of employee completion.

To apply for a public safety grant from the Office of the Governor, a local

government would have to submit with the grant application a written certification of compliance with cybersecurity training requirements for its employees and officials.

If the Governor's Criminal Justice Division determined that a local government awarded a grant had not complied with the required cybersecurity training, the local government would have to pay the grant amount back to the state and would be ineligible for another grant for two years. The bill would apply only to a grant application submitted on or after September 1, 2021.

The bill would require a state agency's strategic plan to include a written certification of compliance with cybersecurity training requirements for the agency's employees and officers and certain state contractors. This provision would apply only to a strategic plan submitted on or after January 1, 2022.

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, 2021.

SUPPORTERS SAY:

CSHB 1118 would continue efforts to minimize the state's cybersecurity risk and decrease points of vulnerability to cyber incidents for government data systems.

The 86th Legislature enacted HB 3834 by Capriglione, requiring certain state and local government employees and state contractors to complete annual cybersecurity training. In implementing the bill, some have noted a number of issues that need to be addressed, including the inconsistency of the training requirement for local government employees and elected officials and of the requirement for state agencies and local governments. CSHB 1118 would address these issues by applying the training requirements uniformly within local governments and across state agencies and local governments.

The bill also would reduce the likelihood of malicious attempts to exploit

cybersecurity weaknesses in personnel by including mechanisms to ensure compliance with cybersecurity training requirements. Local governments seeking public safety grants from the Office of the Governor would have to certify compliance with the training requirement in the grant application process, which would be an effective compliance mechanism as most local governments apply for these grants.

By requiring full local government compliance for grant eligibility, the bill would signal the importance of cyber hygiene; it only takes one employee clicking on one bad link to risk all of a local government's systems. The bill also would account for certain situations in which a local government might have challenges reaching 100 percent compliance, such as having employees on leave.

The bill enhances Department of Information Resources (DIR) oversight of cybersecurity training programs by removing the ability for certain local governments to offer their own programs. Since few local governments have strong cybersecurity infrastructure, they are better served by selecting a DIR-approved training program instead of conducting the training in-house.

CRITICS SAY:

While there should be an enforcement mechanism to ensure compliance with cybersecurity training requirements, tying 100 percent compliance to eligibility for public safety grants unfairly could put important funding for local governments at risk. Under the bill, if one local government employee did not satisfy the training requirement, grant funding would be in jeopardy. Instead, the bill should provide a realistic percentage threshold for compliance, such as 75 or 80 percent, instead of requiring full compliance.