BILL ANALYSIS

C.S.H.B. 2401
By: Deshotel
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

There are concerns that some state employees are not adequately trained and may be vulnerable to a cybersecurity attack. C.S.H.B. 2401 seeks to address these concerns by requiring certain executive branch state agency employees to undergo cybersecurity awareness training.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 2401 amends the Government Code to require each executive branch state agency, other than a public institution of higher education, to require all agency employees who have access to the agency's network or online systems, including email or Internet access, to complete training on cybersecurity awareness. The bill sets out the required components of that training and requires the training to be designed, administered, and maintained by a third-party vendor that meets certain qualifications established by the bill.

EFFECTIVE DATE

September 1, 2019.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 2401 may differ from the original in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute makes revisions to conform to certain bill drafting conventions.

The substitute limits the applicability of the its provisions to executive branch state agencies, other than a public institution of higher education.

The substitute revises the required qualifications for the third-party vendor that designs, administers, and maintains the training.

The substitute does not include a provision expressly requiring the training to include training on information governance, privacy, acceptable use, records management, password management,

open records, spam, electronic mail and phishing, spear phishing, computer viruses and malware, ransomware, social engineering, data management, external or removable media, safe Internet habits, impersonation, improper usage, physical security, mobile data, and incident response.