BILL ANALYSIS

C.S.H.B. 1421
By: Israel
Elections
Committee Report (Substituted)

BACKGROUND AND PURPOSE

It has been noted that the study the legislature asked the secretary of state to conduct regarding cyber attacks on election infrastructure has been completed and the report with recommendations has been issued. C.S.H.B. 1421 seeks to implement some of those recommendations to provide greater cybersecurity for voting systems in Texas.

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 rulemaking authority is expressly granted to the secretary of state in SECTION 1 of this bill.

ANALYSIS

C.S.H.B. 1421 amends the Election Code to require the secretary of state to adopt rules defining classes of protected election data and establishing best practices for identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems. The bill defines "election data" as information that is created or managed in the operation of an election system and "election system" as a voting system and the technology used to support the conduct of an election, including the election data processed or produced in the course of conducting an election. The bill defines "county election officer" as an individual employed by a county as an elections administrator, voter registrar, county clerk, or other officer with responsibilities relating to the administration of elections. The bill requires the secretary of state to offer training on best practices to all appropriate personnel in the secretary of state's office on an annual basis and to county election officers in Texas on request. The bill requires the secretary of state, if the secretary of state becomes aware of a breach of cybersecurity that impacts election data, to notify the members of the standing committees of each house of the legislature with jurisdiction over elections immediately.

C.S.H.B. 1421 requires a county election officer to request training on cybersecurity from the secretary of state and on an annual basis from another provider of cybersecurity training if the county election officer has available state funds for that purpose. The bill requires a county election officer to request an assessment of the cybersecurity of the county's election system from a provider of cybersecurity assessments if the secretary of state recommends an assessment and the necessary funds are available. The bill requires a county election officer, if the officer becomes aware of a breach of cybersecurity that impacts election data, to notify the secretary of state immediately. The bill requires a county election officer, to the extent that state funds are available for the purpose, to implement cybersecurity measures to ensure that all devices with access to election data comply to the highest extent possible with the rules adopted by the secretary of state under the bill's provisions.

EFFECTIVE DATE

September 1, 2019.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 1421 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 extends the cybersecurity duties for a voter registrar or county clerk to a county election officer, defined by the substitute as an individual employed by a county as an elections administrator, voter registrar, county clerk, or other officer with responsibilities relating to the administration of elections.

The substitute changes the required rules adopted by the secretary of state to include the adoption of rules defining classes of protected election data and to specify that the best practices rules are those identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems.

The substitute includes a requirement for a county election officer to request a cybersecurity assessment.