HOUSE
RESEARCH
ORGANIZATION bill analysis 4/15/2019

HB 1421 (2nd reading)
Israel, et al.
(CSHB 1421 by Klick)

SUBJECT: Requiring election officials to participate in cybersecurity measures

COMMITTEE: Elections — committee substitute recommended

VOTE: 7 ayes — Klick, Cortez, Bucy, Burrows, Cain, Fierro, Israel

2 nays — Middleton, Swanson

WITNESSES: For — Heather Hawthorne, County and District Clerks' Association of Texas; Brian Engle, CyberDefenses; (*Registered, but did not testify*: Joyce Hudman and Jennifer Lindenzweig, County and District Clerk's Association of Texas; Damon Fleury, CyberDefenses; Cinde Weatherby, League of Women Voters of Texas; Fatima Menendez, Mexican American Legal Defense and Education Fund; Lon Burnam, Public Citizen; Chris Davis, Texas Association of Elections Administrators; Windy Johnson, Texas Conference of Urban Counties; Glen Maxey, Texas Democratic Party; Daniel Gonzalez and Julia Parenteau, Texas Realtors; Aryn James, Travis County Commissioners Court; Idona Griffith)

Against — Alan Vera, Harris County Republican Party Ballot Security Committee; David Carter; Ed Johnson; (*Registered, but did not testify*; Daniel Greer, Direct Action Texas; Russell Hayter)

On — Keith Ingram, Texas Secretary of State

DIGEST: CSHB 1421 would require certain Secretary of State's Office personnel and county election officers to participate in cybersecurity trainings and assessments related to the security of election infrastructure.

Secretary of state. The secretary of state would be required to define classes of protected election data and establish best practices for identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems. The secretary of state would train appropriate personnel in the Secretary of State's Office on best practices annually and train county election officers upon request.

If the secretary of state became aware of a cybersecurity breach that impacted election data, the secretary would be required immediately to notify the appropriate legislative committees with jurisdiction over elections.

County election officers. County election officers would be required to request cybersecurity training from the secretary of state and, on an annual basis, another provider of cybersecurity training if the county election officer had available state funds for that purpose.

County election officers would be required to request assessments of their election systems if the secretary of state recommended them and the necessary funds were available. The officers would have to immediately notify the secretary of state if there was a cybersecurity breach that impacted election data.

County election officers would be required to implement cybersecurity measures to ensure that all devices with access to election data complied with the cybersecurity rules adopted by the secretary of state, to the extent that state funds were available.

The bill would take effect September 1, 2019.

SUPPORTERS SAY:

CSHB 1421 would strengthen the state's election infrastructure by requiring all counties to participate in cybersecurity training and risk assessments of their work environments if the necessary funds were available. The bill would extend the participation requirements to some counties that previously had declined to participate in such programs offered by the secretary of state because they did not know how they would pay to fix problems that arose or deemed themselves not vulnerable to attacks.

The bill would not place a financial burden on counties because federal funds received in connection with the federal Help America Vote Act are earmarked for cybersecurity purposes through the Secretary of State's Office. Many cybersecurity programs currently are offered to counties free of charge using this funding. The bill would help reduce the risk of data breaches and other cybersecurity incidents that could present significant costs.

OPPONENTS SAY:

CSHB 1421 would require the state to pay for unnecessary cybersecurity trainings and assessments. Election systems are not connected to the internet, and the state's election system has never been hacked. Voter rolls are connected to the internet, but the information contained in voter rolls is largely public information already.