BILL ANALYSIS

C.S.H.B. 1452
By: Blanco
Government Transparency & Operation
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Interested parties assert that the protection of election infrastructure is important. C.S.H.B. 1452 seeks to assist with such protection by requiring the secretary of state to conduct a study regarding cyber attacks on election infrastructure.

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. 1452 amends the Election Code to require the secretary of state, not later than December 1, 2018, to conduct a study regarding cyber attacks on election infrastructure, to prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election, to prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under state public information law, and to submit a copy of the public summary report and a general compilation of the confidential report that does not contain any information the release of which may compromise any election to the standing committees of the legislature with jurisdiction over election procedures. The bill requires the study to include an investigation of vulnerabilities and risks for a cyber attack against a county's voting system machines or the list of registered voters, information on any such attempted cyber attack, and recommendations for protecting such machines and list from a cyber attack. The bill authorizes the secretary of state, using existing resources, to contract with a qualified vendor to conduct the study. These provisions expire January 1, 2019.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2017.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 1452 may differ from the original in minor or nonsubstantive ways, the following comparison is organized and formatted in a manner that indicates the substantial differences between the introduced and committee substitute versions of the bill.

INTRODUCED	HOUSE COMMITTEE SUBSTITUTE
SECTION 1. Chapter 31, Election Code, is amended by adding Section 31.013 to read as follows:	SECTION 1. Chapter 276, Election Code, is amended by adding Section 276.011 to read as follows:
Sec. 31.013. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall	Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall:
conduct a study regarding cyber attacks on election infrastructure	(1) conduct a study regarding cyber attacks on election infrastructure;
and shall report the study's findings to the standing committees of the legislature with jurisdiction over election procedures.	(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;
	(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552, Government Code; and
	(4) submit a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election to the standing committees of the legislature with jurisdiction over election procedures.
The study shall include:	(b) The study must include:
(1) an investigation of vulnerabilities and risks for a cyber attack against voting system machines, the list of registered voters, and election administrators' websites;	(1) an investigation of vulnerabilities and risks for a cyber attack against a county's voting system machines or the list of registered voters;
(2) information on any attempted cyber attack on voting system machines, the list of registered voters, and election administrators' websites; and	(2) information on any attempted cyber attack on a county's voting system machines or the list of registered voters; and
(3) recommendations for protecting voting system machines, the list of registered voters, and election administrators' websites from a cyber attack.	(3) recommendations for protecting a county's voting system machines and list of registered voters from a cyber attack.
(b) In conducting the study required by this section, the secretary of state may consult with any state agency with appropriate expertise, including the Department of Public Safety and the Department of Information Resources.	(c) The secretary of state, using existing resources, may contract with a qualified vendor to conduct the study required by this section.
(c) This section expires January 1, 2019.	(d) This section expires January 1, 2019.
SECTION 2. This Act takes effect immediately if it receives a vote of two-thirds of all the members elected to each house, as provided by Section 39, Article III, Texas Constitution. If this Act does not receive the vote necessary for immediate	SECTION 2. Same as introduced version.

effect, this Act takes effect September 1, 2017.