By: Hall S.B. No. 78

A BILL TO BE ENTITLED

AN ACT

relating to the security of election systems.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 279, Election Code, is amended by amending Sections 279.002 and 279.003 and adding Sections 279.004 and 279.005 to read as follows:

Sec. 279.002. ELECTION CYBERSECURITY: SECRETARY OF STATE. (a) The secretary of state shall adopt rules defining classes of protected election data and establishing best practices for identifying, [~~and~~] reducing, and eliminating the risk to the electronic use, storage, and transmission of election data and the security of election systems, including:

(1) methods of encrypting data at rest and during transmission; and

(2) restricting access to sensitive election data to only users with a specific need to access that data.

(a-1) The secretary of state shall appoint a dedicated cybersecurity expert to implement cybersecurity measures to protect all election data and other election-related data held by the state or a county in the state, including technology that blocks, notifies, and reports on unauthorized attempts to access or transfer data.

(b) The secretary of state shall direct the cybersecurity expert to offer training on best practices:

(1) on a biennial [~~an annual~~] basis, to all appropriate personnel or contractors with [~~in~~] the secretary of state's office with access to sensitive election data; and

(2) on request, to county election officers and any employees or contractors of the county election officers with access to sensitive election data [~~in this state~~].

(b-1) Access to sensitive election data shall be revoked for any employee or contractor that is required to receive training under Subsection (b) but does not complete the training.

(c) If the secretary of state becomes aware of a breach of cybersecurity that impacts election data, the secretary shall immediately notify the governor, lieutenant governor, speaker of the house of representatives, and members of the standing committees of each house of the legislature with jurisdiction over elections. The secretary shall direct the cybersecurity expert to conduct an investigation of the breach and report any findings to the governor, lieutenant governor, speaker of the house of representatives, and members of the standing committees of each house of the legislature with jurisdiction over elections.

(d) During an investigation conducted under Subsection (c), access to the election system is restricted to only individuals designated by the secretary of state until the standing committees confirm that the breach has been mitigated.

(e) If the investigation under Subsection (c) reveals that individuals' personal data has been breached, the secretary of state shall promptly notify the affected individuals by written letter of the occurrence and extent of the breach.

(f) The secretary of state, in cooperation with the cybersecurity expert, shall contract with a provider of cybersecurity assessments to biennially conduct an assessment of the cybersecurity of the state's election system.

(g) The cybersecurity expert shall implement cybersecurity measures to ensure that all devices with access to election data held by the state comply to the highest extent possible with rules adopted by the secretary of state under Subsection (a).

Sec. 279.003. ELECTION CYBERSECURITY: COUNTY ELECTION OFFICERS. (a) A county election officer shall biennially [~~annually~~] request training on cybersecurity from the cybersecurity expert appointed by the secretary of state under Section 279.002. The secretary of state shall pay the costs associated with the training with available state funds.

(b) A county election officer shall contract with a provider of cybersecurity assessments to biennially conduct [~~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~~].

(b-1) The county election officer shall deliver a report on any recommended improvements to the county's election system by the assessment conducted under Subsection (b) to the secretary of state.

(c) If a county election officer becomes aware of a breach of cybersecurity that impacts election data, the officer shall immediately notify the secretary of state. If the secretary of

state is made aware of a breach under this section, access to sensitive election data in the county shall be restricted to specific personnel during an investigation by the secretary.

(d) A [~~To the extent that state funds are available for the purpose, a~~] county election officer shall implement cybersecurity measures to ensure that all devices with access to election data comply to the highest extent possible with rules adopted by the secretary of state under Section 279.002.

Sec. 279.004. INTERNAL PERSONNEL VIOLATION. If a data breach under this section is conducted by an employee of the secretary of state's or county election officer's office, the employee may not be provided access to election-related data until an investigation under this section is concluded. If an investigation determines that the employee intentionally breached an election system, the secretary of state may pursue all available legal remedies against the employee, including criminal prosecution.

Sec. 279.005. COMPUTER NETWORK CONNECTIVITY. (a) Except as expressly authorized by this code, an election system that is capable of being connected to the Internet or any other computer network may not be used in an election held in this state, except for the use of a visible wired connection to an isolated local area network within the building.

(b) The cybersecurity expert appointed by the secretary of state under Section 279.002 shall annually verify compliance with this section by each county conducting an election in this state.

SECTION 2. Section 123.034, Election Code, is amended to

read as follows:

Sec. 123.034. MAINTENANCE AND STORAGE OF EQUIPMENT. (a) The governing body of a political subdivision shall provide for the proper maintenance and storage of the equipment that the subdivision acquires for use in the operation of a voting system.

(b) Equipment used in the operation of a voting system must have a documented chain of custody and be stored in a locked facility with video surveillance monitoring the storage facility at all times.

SECTION 3. As soon as practicable after the effective date of this Act, the secretary of state shall:

(1) adopt the rules required by Section 279.002(a), Election Code, as amended by this Act; and

(2) appoint a cybersecurity expert in accordance with Section 279.002(a-1), Election Code, as added by this Act.

SECTION 4. This Act takes effect September 1, 2025.