BILL ANALYSIS

C.S.S.B. 820
By: Nelson
Public Education
Committee Report (Substituted)

BACKGROUND AND PURPOSE

As public school districts move from paper files to electronic systems, student and employee data is a potential target for cyber criminals. The Texas Education Agency data security advisory committee recently recommended certain legislative priorities to better protect such data. C.S.S.B. 820 seeks to implement advisory committee recommendations by requiring each district to adopt a cybersecurity policy and designate a cybersecurity coordinator and by establishing certain reporting requirements.

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.S.B. 820 amends the Education Code to require each public school district to adopt a cybersecurity policy to secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents, determine cybersecurity risk, and implement mitigation planning. The bill prohibits a district's cybersecurity policy from conflicting with the information security standards for public institutions of higher education adopted by the Department of Information Resources under the Information Resources Management Act and under statutory provisions relating to the Texas computer network security system.

C.S.S.B. 820 requires the superintendent of each district to designate a cybersecurity coordinator to serve as a liaison between the district and the Texas Education Agency (TEA) in cybersecurity matters. The bill requires the coordinator to report to TEA any cyber attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as defined by the Identity Theft Enforcement and Protection Act as soon as practicable after the discovery of the attack or incident.

EFFECTIVE DATE

September 1, 2019.

COMPARISON OF SENATE ENGROSSED AND SUBSTITUTE

While C.S.S.B. 820 may differ from the engrossed in minor or nonsubstantive ways, the following summarizes the substantial differences between the engrossed and committee substitute versions of the bill.

The substitute replaces the requirement for a district to develop and maintain a cybersecurity framework with a requirement to adopt a cybersecurity policy. The substitute replaces the requirement for a district's cybersecurity framework to be consistent with certain information security standards with a prohibition against the district's cybersecurity policy conflicting with those standards.

The substitute includes a specification that the cybersecurity incidents against a district's cyberinfrastructure that the district is required to report to TEA are those that constitute a breach of system security as defined by the Identity Theft Enforcement and Protection Act.