BILL ANALYSIS

Senate Research Center
86R7097 TSS-D

S.B. 820
By: Nelson
Education
4/3/2019
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

As school districts move from paper files to computers and data systems, valuable student and employee data is a target for cyber criminals. The Data Security Advisory Committee (DSAC) recently put together a list of priorities for the upcoming session. The DSAC provides guidance to Texas education communities (K-12), maximizing collaboration and communication regarding information security issues and resources.

S.B. 820 seeks to implement recommendations from the DSAC to protect vulnerable student and employee data from cyber criminals.

As proposed, S.B. 820 amends current law relating to a requirement that a school district develop and maintain a cybersecurity framework.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter D, Chapter 11, Education Code, by adding Section 11.175, as follows:

Sec. 11.175. DISTRICT CYBERSECURITY. (a) Defines "cyber attack" and "cybersecurity."

(b) Requires each school district to develop and maintain a cybersecurity framework for the securing of district cyberinfrastructure against cyber attacks and other cybersecurity incidents and cybersecurity risk assessment and mitigation planning.

(c) Requires a school district's cybersecurity framework to be consistent with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 (Information Resources) and 2059 (Texas Computer Network Security System), Government Code.

(d) Requires the superintendent of each school district to designate a cybersecurity coordinator to serve as a liaison between the district and the Texas Education Agency (TEA) in cybersecurity matters.

(e) Requires the district's cybersecurity coordinator to report to TEA any cyber attack, attempted attack, or other cybersecurity incident against the district cyberinfrastructure as soon as practicable after the discovery of the attack or incident.

SECTION 2. Effective date: September 1, 2019.