BILL ANALYSIS

C.S.H.B. 3000
By: Talarico
Public Education
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Concerns have been raised regarding the high incidence of recent major breaches involving student and teacher personal information in Texas. C.S.H.B. 3000 seeks to combat this issue by ensuring that all students, educators, and district employees are notified when their data may have been accessed illicitly and by requiring the establishment of a database that contains information regarding each reported district data breach.

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 rulemaking authority is expressly granted to the commissioner of education in SECTION 1 of this bill.

ANALYSIS

C.S.H.B. 3000 amends the Education Code to require a public school district to provide written notice to a parent of or person standing in parental relation to a student enrolled in the district of a district data breach involving the student's information not later than the 30th day after the date on which the district becomes aware of the data breach. The bill defines "data breach" and sets out the required contents of the notice. The bill requires a district to submit to the Texas Education Agency (TEA) a report on a district data breach not later than the 60th day after the date the district becomes aware of the data breach and sets out the required contents of the report. The bill establishes that the following information included in the report is confidential and not subject to disclosure under state public information law:

- detailed information regarding the nature of the data breach; and
- a detailed description of any action taken or planned to be taken by the district to reduce damage as a result of the data breach or to prevent another data breach.

C.S.H.B. 3000 requires TEA to establish and maintain an electronically searchable database that contains information regarding each reported district data breach. The bill requires the database to contain certain publicly accessible information for each data breach and also to contain for each data breach the confidential information included in the district's report to TEA. The bill requires TEA to ensure that only a school administrator may access the confidential information contained in the database. The bill authorizes the commissioner of education to adopt rules as necessary to implement the bill's provisions relating to student data security.

C.S.H.B. 3000 explicitly subjects an open-enrollment charter school to a prohibition, restriction, or requirement imposed by the bill's provisions relating to student data security or a rule adopted under those provisions.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2019.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 3000 may differ from the original in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute clarifies that the sensitive, protected, or confidential student information referenced in the definition of "data breach" is classified as such as provided by state or federal law.

The substitute changes the deadline for a public school district to provide written notice to a parent of or person standing in parental relation to a district student of a data breach involving the student's information from not later than the 10th day after the date on which the district becomes aware of the breach to not later than the 30th day after that date. The substitute changes the deadline for a district to submit to TEA a report on a district data breach from not later than the 10th day after the date the district becomes aware of the data breach to not later than the 60th day after that date.

The substitute specifies that the contents of the required notice and report of a district data breach describing any action taken or planned to be taken by the district to prevent another data breach include adopting a student privacy pledge.