SUBJECT: Establishing requirements for student data security in public schools

COMMITTEE: Public Education — committee substitute recommended

VOTE: 11 ayes — Huberty, Bernal, Allen, Ashby, K. Bell, M. González, K. King, Meyer, Sanford, Talarico, VanDeaver

0 nays

2 absent — Allison, Dutton

WITNESSES: For — (*Registered, but did not testify*: Jacquie Benestante, Autism Society of Texas; Chris Masey, Coalition of Texans with Disabilities; Jolene Sanders, Easterseals Central Texas; Lonnie Hollingsworth, Texas Classroom Teachers Association; Linda Litzinger, Texas Parent to Parent; Kyle Ward, Texas PTA; Jen Ramos, Texas Young Democrats; Kyle Piccola, The Arc of Texas; Drew Scheberle, The Greater Austin Chamber of Commerce; and 12 individuals)

Against — (*Registered, but did not testify*: Bill Kelberlau)

On — (*Registered, but did not testify*: Eric Marin and Melody Parrish, Texas Education Agency)

BACKGROUND: Interested parties have raised concerns about breaches involving student and teacher personal information in Texas.

DIGEST: CSHB 3000 would require a public school district or an open-enrollment charter school to provide written notice to a parent or guardian of a student enrolled in the district or charter school of a school district data breach involving the student's information by the 30th day after the date on which the school became aware of the breach.

The notice would have to include a description of the type of information that was the subject of the breach as well as a general description of any action taken or planned to be taken by the district to reduce resulting

damage and prevent another breach.

By the 60th day after the school learned of the breach, the school would be required to submit to the Texas Education Agency (TEA) a report that included:

- detailed information regarding the nature of data breach;
- the number of students affected;
- a description of the type of information that was the subject of the breach; and
- a detailed description of any action taken or planned to be taken by the district to reduce damage resulting from the breach and to prevent another data breach.

TEA would be required to establish and maintain an electronically searchable database that contained information on each reported school district data breach.

For each school district data breach, the database would have to include publicly accessible information about the school district at which the data breach occurred and the number of students affected.

The database also would be required to include detailed information on the nature of the breach and the school's response. TEA would have to ensure that only school administrators could access this information, and the information would not be subject to disclosure under state public information laws.

The commissioner of education could adopt rules as necessary to implement the provisions of the bill.

The bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2019.

NOTES: According to the Legislative Budget Board, the bill would have a negative

financial impact of about $1.3 million to general revenue related funds through fiscal 2020-21. Following that, the bill would continue to have a negative impact of $216,000 per fiscal year.