Ohio Legislative Service Commission

Jason Phillips

Fiscal Note & Local Impact Statement

Bill: Sub. H.B. 181 of the 130th G.A. **Date**: December 5, 2013

Status: As Reported by House Education **Sponsor**: Rep. Brenner

Local Impact Statement Procedure Required: No

Contents: Management of the statewide education data repository and personally identifiable information of students

State Fiscal Highlights

- The bill requires the Ohio Department of Education (ODE) to perform a number of duties in relation to the statewide education data repository, the statewide longitudinal data system (SLDS).
- ODE indicates that the bill's various monitoring, data collection documentation, and reporting functions will result in the need for a new full-time position with payroll and fringe benefit costs estimated at around $100,000 annually.
- The bill requires ODE to engage in privacy and security audits as part of a detailed data security plan. ODE estimates that a privacy and security audit program will cost about $175,000 in the first year and $50,000 to $75,000 per year thereafter if audits are conducted on an annual basis.
- The bill may result in the need for enhanced electronic and administrative safeguards. If necessary, ODE estimates software costs to be in the $250,000 to $500,000 range.

Local Fiscal Highlights

- The bill requires each school district board of education to publish on the district's website a list of entities to which directory information was released during the previous school year. This may result in a minimal increase in the administrative burden of each school district.

Detailed Fiscal Analysis

Management of statewide education data repository

The statewide education data repository, Ohio's statewide longitudinal data system (SLDS), combines student data for students in publicly funded early childhood programs, public elementary and secondary schools, and public institutions of higher education using the existing system used by the Ohio Department of Education (ODE) to give each student a unique identifier number. Though the SLDS is physically maintained by ODE, under continuing law its operation is guided by a memorandum of understanding (MOU) between ODE and the Ohio Board of Regents (BOR). The MOU, among other provisions, requires procedures to be in place concerning maintenance of the data in SLDS, specifies the types of research that may be conducted using the data, and requires that the data be managed in a manner that complies with the federal Family Educational Rights and Privacy Act (FERPA), which controls the release of student education records. The bill requires ODE to perform a number of duties to increase the Department's accountability in managing SLDS data. Under the bill, ODE must:

- Develop a detailed data security plan that contains various guidelines, standards, procedures, and policies and provides for privacy and security audits;
- Notify the General Assembly of any additions or changes to the data fields being collected at least 60 days prior to the implementation of those changes;
- Announce any proposed data collection to the general public for a review and comment period of at least 60 days prior to implementing that collection of data;
- By September 1 each year, establish and publish a data inventory and dictionary or index of data elements describing individual student data fields in the SLDS;
- By September 1 each year, develop and publish policies and procedures to be used to maintain compliance with all relevant state and federal privacy laws and policies, including a procedure for notifying parents and students of privacy rights and permitting access to student data only to certain persons;
- By September 1 each year, develop criteria for the approval of research and data requests; and
- Annually report to the Governor and the General Assembly concerning proposed student data elements, changes to existing data collections, an explanation of any exceptions granted by the State Board of Education in

the past year regarding the release of student or redacted data, and the results of privacy compliance and security audits completed in the past year.

Fiscal effects

There are three primary cost drivers associated with these responsibilities: staffing, privacy and security audits, and enhanced safeguards in accessing student data. Other provisions appear to impose no more than an increase in ODE's administrative burden, though the 60-day waiting period before data fields are added or modified may result in delays in the implementation of new legislation. The provisions with a significant fiscal effect are discussed in more detail below.

ODE expects that it will need one new full-time equivalent employee to support the bill's monitoring, data collection documentation, and reporting functions. ODE estimates that the payroll and fringe benefit costs associated with this new position will be around $100,000 annually.

The bill's requirement to engage in privacy and security audits as part of the detailed data security plan is also expected to increase ODE's costs. In general, a privacy audit evaluates an organization's compliance with privacy responsibilities while a security audit evaluates access control procedures and systems to determine the level of susceptibility to unauthorized individuals. Overall, the cost of these audits will vary depending on the rates charged to perform the audits as well as their scope and frequency. ODE estimates a privacy and security audit program to cost about $175,000 in the first year and $50,000 to $75,000 per year thereafter, if audits are conducted on an annual basis.

There may also be some potentially significant costs to enhance ODE's safeguards with respect to student data, as the bill's detailed data security plan requires development of guidelines for authorizing access to SLDS data and data security policies. While ODE has many electronic and administrative safeguards in place already, it may be that ODE needs to implement additional safeguards. If such enhancements are determined to be necessary, ODE estimates that the cost to purchase the requisite software to implement the safeguards will be in the $250,000 to $500,000 range.

Online listing of directory information releases

The bill requires each school district board of education to publish on the district's website a list of entities to which directory information was released during the previous school year. Unlike other education records, directory information may be disclosed by schools without written consent of the student's parent or the student, unless the parent or student opts to have the student's information withheld from disclosure. This provision may result in a minimal increase in the administrative burden of each school district.

Personally identifiable information releases

The bill contains several provisions related to the personally identifiable information of students. First, the bill prohibits ODE from releasing personally identifiable information except in statutorily prescribed limited circumstances or when necessary to comply with all relevant laws and rules including FERPA. Except in certain limited circumstances, ODE does not have access to personally identifiable student data, as current law requires the Department to engage an independent contractor to assign each student enrolled in a public school a unique identifier number, often called the student's "SSID." Public schools use this number to report student data to the Department. Further, ODE aggregates student-level data before it is released.

Second, the bill prohibits public schools from submitting, without consent, personally identifiable information of any student to the federal government unless the school's governing board has adopted a resolution approving the submission, though public schools will still need to comply with FERPA. The bill requires school governing boards adopting such resolutions to develop and publish criteria, policies, and procedures for the submission of the data in compliance with FERPA and other relevant privacy laws and policies. Although the adoption of a resolution by a school's governing board and the resulting work associated with developing and publishing criteria, policies, and procedures may increase the administrative burden of the board, it is unlikely that many resolutions will need to be adopted, if any. As noted above, student-level data typically is sent to ODE, which aggregates it before it is sent to the federal government, or such data is provided in accordance with existing FERPA exceptions.

HB0181HR.docx / lb