Oregon Department of Education

John A. Kitzhaber, MD, Governor

Office of the Deputy Superintendent
255 Capitol St NE
Salem, OR 97310
Voice: 503-947-5600
Fax: 503-378-5156

HB 2710: Privacy Risk Assessments
House Education Committee
February 13, 2015

Chair Doherty, members of the committee, for the record I am Ben Tate, Chief Information Officer at the Oregon Department of Education. I am here today to testify on HB 2710 which directs the Department of Education to issue privacy risk assessments of any data system, program, or contract involving student education records.

Background:
The safety, accuracy, and security of student education records is a critically important mission for the Oregon Department of Education. ODE has created a comprehensive Information Security and Privacy Program (http://goo.gl/XmbtoC) that incorporates security protections required by state and federal laws, state policy, and best business practices.

There are three primary risks to student data: human error and misuse; unsound processes and policies; and technology failures.

To reduce the potential for human error, ODE provides annual mandatory information security and privacy fundamentals training; provides regular security and privacy newsletters and security bulletins , includes security and privacy information in ODE newsletters; orient all new ODE employees on their responsibilities regarding information security and privacy; and provides targeted information security training for specific groups.

To ensure ODE and schools are using the most up-to-date processes and policies, we monitor changes in state and federal regulations and update our policies in response. The Family Education Rights Privacy Act (FERPA) was recently amended to clarify the handling of student data in the construction and use of statewide longitudinal data systems, for instance. ODE also provides communication as new security issues are discovered to ensure appropriate actions are taken. ODE has implemented a number of policies around this issue, including the acceptable use of personally identifiable student information. ODE conducts security audits against systems to make sure access and rights are appropriate and conducts security reviews of any procurements and contracts involving data exchange, data access, and research.

The technology element focuses on technologies that support the protection of the confidentiality, integrity, and availability of the data and the systems we are responsible for securing. A short list of the security measures taken to protect student data include encryption of data, firewalls, limited access to data, regular patching of servers, laptops and desktops, and backup and offsite secure storage.

In addition to maintaining a comprehensive information security and privacy program for the department, ODE worked with districts and ESDs to launch a statewide Education Information Security Council, under the umbrella of the IT Manager's advisory council.

Issue:

Ensuring the security and privacy of student education records.

Legislation:

HB 2710 seeks to direct the Department of Education to issue privacy risk assessments to any data systems, programs or contracts involving student education records.

Concerns:

The scope of this bill is very broad. The department estimates that (on average) each school district has 20-40 contracts, systems or programs to be audited. These contracts, systems and programs also change on a frequent basis, meaning that the amount of work necessary to provide these audits would require a large amount of staff and funding . ODE is not in the audit business, it would not be appropriate for us to build an internal audit shop for this work. We believe this function would be more appropriate for the Secretary of State's Audits Division.

This runs counter to the direction ODE has taken the last few years. We have been striving to move from a compliance agency to a support agency. This is would be a large compliance role. We believe there would be more lasting results to educate school districts and ESDs personnel on student data privacy. Given the rapid rate of technical change, educating School District and Education Service District personnel on the principles of responsible student data management, will help them navigate these waters on their own and the department will provide technical support as needed.

Fiscal:

As written, we estimate approximately 50 FTE would be necessary to handle this workload.