Joyce Popp
Chief Information Officer
Idaho State Department of Education
June 25, 2014
"How Data Mining Threatens Student Privacy"

Thank you Chairmen, ranking members and committees members for allowing me time to address you on the important issue of student data privacy. It is truly an honor to have this opportunity to discuss Idaho's practices around collecting and protecting student data. In education, all teachers should have access to meaningful data to support their instructional practices; data that is collected is now available to all educators, both administration and teachers in Idaho to support them in making data driven decisions to impact student achievement. We will continue our efforts with the understanding that student level data must be respected and protected while also acknowledging that student information is a vital resource for teachers and school staff in their educational planning. In Idaho, we have been working diligently to find the proper balance of strong data security policy while also supporting stakeholders. Data stewardship has been a talking point within the Idaho State Department of Education for quite some time, teaching and encouraging school districts leaders to adopt equally as strong data collecting and management policies. This process must not only happen at the state level, but also at the school district and down to the individual teacher level.

I have been with the Idaho State Department of Education for 5 years and in the capacity of Chief Information Officer for the past several years. My background is largely in the private sector, working in Senior Management for several Fortune 500 companies, dealing in the Information Systems and Information Technology area where infrastructure, eCommerce, data systems, and data security was a key focal point. Data usage and security of information in the private sector is of the upmost of importance just as it is in the education world. Through this experience I have a working knowledge of data systems and how essential it is to protect student level data and ensure student data privacy. All companies in the private sector secure their customer's data and

likewise, state and local educational institutions must make the same or greater efforts to protect student data. We live in a world where cyber threats and attempts to breach data systems are prevalent, and we must make every effort to protect this data but also to be vigilant in our data use efforts. As we all understand however, data security is not the same as data privacy.

Idaho collects student level data for reporting purposes while also supporting state and federal programs. We do not want to be collecting data for data sake, however we want to be collecting only data that is clearly needed to improve educational outcomes for the students of Idaho. Currently, the State of Idaho collects attendance data for each day or portion of a day a student is in class as this is used for funding purposes and program participation; yet the state does not collect a specific reason for an absence as this is currently not a data element necessary for program or funding calculations. We collect data at the student level as all data must be repeatable, defensible, and auditable. All of the data elements that have been, and that are currently being collected have been published on the public website and made available for district personnel and patrons. Along with this information our department publishes why we collect this data, down to each individual data element. Over the past four years we have been receiving data from our school districts via secure measures. We are constantly auditing and evaluating the data we collect, and how we collect it to ensure that technology best practices are employed. Through this refinement process, we have improved our efforts in supporting teachers and school administrators with quality, timely data. Also in this process, we worked with our Idaho legislators and other stakeholders to create a piece of legislation that ensures that our educational institutions not only have the policies and protocols to ensure data security but also data privacy. Included in the legislation, individuals are held accountable for improper handling and use of student level data.

For years, school districts and state agencies have diligently followed the guidelines of the Family Educational Rights and Privacy Act (FERPA) which provides guidance on disclosure of personally identifiable information (PII) from educational records. Not only has Idaho followed these guidelines, but we have taken a conservative approach in the

interpretation of FERPA to safeguard student level data. Educational stakeholders and their elected officials in Idaho continue their efforts to work together in order to ensure student data is protected. This is evident by the crafting of Senate Bill 1372 during the 2014 legislative session, a student data privacy bill. Idaho utilized information and recommendations put out by the Privacy Technical Assistance Center (PTAC) through the U.S. Department of Education. As stated within the Data Governance and Stewardship document provided by PTAC, "successful data management requires a proactive approach to addressing stakeholders' needs for high quality data, while protecting the privacy of individual respondents."

The intent of Senate Bill 1372, known as the Student Data Accessibility, Transparency and Accountability Act of 2014, is to ensure that student information is safeguarded and that privacy is honored, respected and protected while also acknowledging that student information is a vital resource for teachers and school staff in their educational planning. This bill also provides specific definitions and guidelines authorizing access to student data systems and to individual student data, hence our continued focus on data stewardship. The bill also includes language addressing a penalty not to exceed $50,000 if anyone within the agencies, districts or public charters fail to protect the data and a breach of student level data occurs or is released without proper authorization. In addition to addressing use, protection and breaches of data, each public school district or charter school is required to adopt data protection and privacy policies and guidelines. Awareness is a key component to the adoption of this new law, and district personnel have been notified and made aware of this responsibility. Presentations are being conducted around the state to emphasize the details and importance of the new law.

We are also aware that not all school districts have the capacity to write data security policy; in knowing this, the bill also calls for the Idaho State Board of Education to develop a model policy for school districts and public charter schools that will govern data collection, access, security and use of such data. The Idaho State Board of

Education is currently working on the model policy and will have it available for all school districts and public charters this summer.

I have made a concerted effort to provide awareness meetings to all staff within the Idaho State Department of Education. In these meetings I discuss the intent of Senate Bill 1372, and the level of accountability, roles and liabilities that state employees will be required to adopt as well as our obligation to educate our districts and schools of their responsibilities. Divisions within the agency handle different types of data; however an example that has been used is Child Nutrition Programs. The United States Department of Agriculture (USDA) requires a specific "need to know" basis to access free and reduced price meal eligibility information. Under the rule of the USDA, state agencies, districts and public charters must ensure that data systems, records and other means of accessing a student's eligibility status are limited. The "need to know" thought process is being adopted by the Idaho State Department of Education for all employees who handle or might have access to student level data.

As Idaho has many rural and even remote school districts, we also take into consideration the population size whenever aggregating data. We have methods to mask small cell size and ensure that data is not personally identifiable even when aggregated.

Along with this thought process is also gaining the knowledge of proper transfer of student level data. For example, we have adopted policies for data governance that prohibits student level data being passed by email. Employees and districts have received training on encryption and other methods of data privacy and security. Sensitive information is more properly transferred using password and data encryption, through a Secure File Transfer Protocol (SFTP), again on a "need to know" basis. Policies have also been adopted to ensure that any contractors or vendors who receive student level data for specific purposes do not use the data outside of the specified use clearly called out in the contract. All contracts, in addition to data use, are required to have specific data destruction and proof of data destruction dates. In a review of prior contractual agreements made with vendors that were up for renewal,

Idaho became aware of verbiage which stated the vendor “owned” the data it was provided. This verbiage is no longer allowed on Idaho State Department of Education contracts and as previously stated we require proof of destruction and the associated dates of the destruction.

The Idaho State Department of Education receives many public records requests and researcher requests to supply student level data. Idaho has put together policies which provide the ability to decline all such requests for student level data. To the individual making the public records request, only aggregate data will be made available. This means data collected or reported at the group, cohort of institutional level only and will not include any personally identifiable information once again taking into consideration small cell sizes within the aggregate data.

Idaho Department of Education has hired cybersecurity experts to constantly monitor and review processes and procedures, including the types of hardware and software programs purchased and deployed within our data center. Data privacy however is not as easily addressed, as it is everyone’s responsibility.

To close, Idaho has and will continue to take the proper steps in implementing data security and policies to protect student level data. It is our responsibility to continually strive to adapt to the constantly changing world of technology and cyber threats; adequate is not enough when dealing with student data privacy. We will continue to better our systems and policies to ensure that student data privacy is not a hope in the state of Idaho, but a reality.

Chairmen, ranking members and committees members, again thank you for this opportunity and I would stand for any questions you may have.