Recommendations on
Data Security and Privacy Protections

Excerpted from the *Data Protections Report* submitted to the U.S. Department of Education's Performance Information Management Service by Highlight Technologies on June 16, 2010

Foreword from the U.S. Department of Education

Given the national interest in protecting the growing amount of student data housed in longitudinal education data systems at all levels, the US Department of Education is seeking to provide resources to assist education agencies in protecting data in longitudinal data systems. Earlier this year the Department engaged a contractor, Highlight Technologies, to produce a report for our Performance Information Management Service on publicly available resources on data security for education data systems. The contractor assembled a group of privacy and security experts to help guide the development of the report. The report will be used as a resource by the Department's forthcoming Privacy Technical Assistance Center, currently being organized by the National Center for Education Statistics and expected to be in operation by late 2010. Based on their research and analysis in the preparation of the report, as well as the input they received from their advisory panel, Highlight Technologies developed a list of recommendations on ways that the Department can address emerging challenges in protecting student data in education data systems. In order to hear from all stakeholders, we are making these recommendations available to the public for review and additional suggestions until August 13, 2010. After that date, the Department will publish responses to the recommendations received.

Recommendations from Highlight Technologies

Overarching Recommendations

Define Data Collection Purposes and Align Security and Privacy Implementation Practices

We recommend that states and school systems be asked to come together, with advice and guidance from the Department, to agree upon what the specific purposes are for collecting student data and how the specific data elements collected can serve those purposes. This understanding can serve as critical input for defining data access and

permissible use.

Aligning those outcomes with Fair Information Practice Principles (FIPPs) and Organization for Economic Co-operation and Development (OECD) Guidelines can provide a comprehensive and methodical framework for assessing data, which can be helpful to strategic planning, decision-making, and resource allocation.

Many on the Expert Advisory Panel indicated the need for a comprehensive approach aligned with the FIPPs.

Develop and Evolve a Dynamic Privacy Knowledge Base (PKB)

We recommend that the Department consider developing a Privacy Knowledge Base (PKB), a dynamic site for assisting states with privacy implementation issues, which could be evolved to capture strategic and tactical privacy information. We envision the PKB as a dynamic knowledge map where states could access resources, tools, discussions, and information on privacy matters as they work to unify their data systems and create their student longitudinal data systems (SLDSs).

The PKB might include resources, timelines, lessons learned, as well as collaborative online discussions organized to address emerging issues and enhance understanding of the challenges. It could serve as a repository of information, populated with studies, white papers, recommendations, reports and findings that could serve as a reference for Department policies and decisions, enabling collaboration and supporting more informed and timely solutions.

The PKB could be crafted to reflect the Department's objectives, interests, and issues specific to SLDSs. Such a resource would allow the Department to address privacy matters systematically, promote transparency in privacy implementation issues, facilitate standards and accountability, encourage collaboration, reduce duplicative efforts, and enhance effectiveness pertaining to privacy implementation initiatives among states.

We are aware of Educause, the non-profit site that supports higher education "by promoting the intelligent use of information technology" (HYPERLINK "http://www.educause.edu/"http://www.educause.edu/). Unlike Educause, which sells institutional and other memberships and offers information and resources on a wide range of IT topics and issues important to higher education, we are recommending a site that, while it might also provide webcasts and toolkits, would restrict the scope of its offerings to security and privacy implementation issues as they pertain to SLDSs. While Educause focuses on some important IT issues, it does not address the matters of concern raised by the current investigation.

We are also aware of the Data Quality Campaign (DQC) (HYPERLINK "http://

www.dataqualitycampaign.org/survey/elements"http://www.dataqualitycampaign.org/survey/elements), a national advocacy group that assists state policymakers with improving and using high-quality education data for improving student achievement. We note that data security and privacy matters are absent from the list of 10 Essential Elements states are advised to use as a measure for building highly effective SLDSs. Although the DQC is not a government organization, its omission of a data security and privacy benchmark does underline the need for more attention to privacy issues, especially since they are driven by law and demand compliance. Developing a PKB would allow the Department to recognize, address, and support the current need.

Provide Guidance on Incident Response Plans

We recommend that the Department provides guidance to states on how to manage breaches of personally identifiable information (PII). Most states have enacted legislation requiring notification of security breaches involving PII, which directly impacts school districts. There are also Federal requirements and guidelines for reporting breaches of PII by or on behalf of the Federal Government. Such guidance could be included in the dynamic PKB explained above.

Create a Leadership Dashboard Space to Enhance Decision-Making

Also as part of the PKB suggested above, we recommend that the Department create an online Leadership Dashboard space to provide a snapshot of current privacy matter implementation status, implementation gaps, and benchmarks that can serve as a roadmap for facilitating policy implementation issues at the state level.

The Leadership Dashboard space could be helpful to the Department by providing evidence for decision-making and for identifying and developing strategies for prioritizing and guiding privacy implementation initiatives. For instance, should the Department decide to move forward with recommendations for benchmarking and online training, the Dashboard would help serve transparency and performance management goals.

There are cost-effective options available for providing such functional solutions that have the potential to impact practices significantly.

Benchmarks

Work with NIST to Develop Recommended Security Controls for Educational Systems Modeled after the NIST Special Publication 800-53

We recommend that the Department reach out to National Institute of Standards and Technology (NIST) to create alliances in order to benefit from the experiences and materials of other organizations. There is significant overlap between Department concerns and issues experienced among other organizations and agencies. Working with NIST to develop recommended security controls for educational systems modeled after the NIST Special Publication 800-53 could allow for security control guidance that is standardized yet specifically tailored to educational systems, enhancing its usefulness to the current context. In addition, a NIST type control structure allows for performance metrics and testing, within a well-known framework, which can be an adaptation of the Federal Certification and Accreditation (C&A) process.

Define a Minimum Standard for Audit Reviews

We recommend that the Department identify a minimum standard for audit reviews; a set of predefined objectives that the review would need to achieve in the review.

Through providing a baseline requirement, states would be able to then modify the audit objectives to fit their individual data warehouses while still being able to be evaluated in relation to other states once the audit report is complete.

Identify and Share Benchmarks for Vendors Housing SLDSs

We recommend that the Department provide states with standards that will allow them to more easily identify appropriate contractors for housing their data systems. Examples of the kinds of benchmarks that might be addressed are: Types and levels of certifications, levels of experience with educational materials, and level of experience and success with security audits.

Detail Benchmarks for Divergent User Group Training

We recommend that the Department detail standards for privacy and security training that could represent a conceptual framework for what different groups of users should know, do, and avoid doing when using SLDSs.

(Then, training driven by these standards could be made public for anyone wanting to become more knowledgeable in the content represented. Much like the Department of Homeland Security Independent Study Program Courses offered for state and local emergency management professionals, this particular self-help privacy and security training could be developed to span learning objectives that range from awareness to demonstrated effectiveness. In other words, the training could be designed so that users could choose to view materials intended to serve awareness; or, they might dive deeper and complete mastery exercises or scenarios to determine how well they can apply new knowledge.)

Education and Training

Develop a Professional Certification through IAPP for Education Privacy (CIPP/ED)

We recommend that the Department work with the International Association of Privacy Professionals (IAPP) to develop a professional certification program for privacy professionals in education (CIPP/ED).

The IAPP is a globally-recognized professional organization dedicated to the education and promotion of the privacy profession. IAPP provides an advanced privacy certification in various specializations including IT (CIPP/IT), Government (CIPP/G), and Canadian Privacy (CIPP/C). Working with IAPP to develop a CIPP/ED certification would leverage the professional organization, promote cross sector exchanges of lessons learned and best practices, and raise the profile of privacy in education systems.

Provide Online Electronic Data Security and Privacy Training to States

We recommend that the Department develop and provide comprehensive online training to states on electronic data security and privacy implementation matters that states could make available to their districts. An investment in online training can support a cohesive implementation of information management, substantially reducing numbers of incidents or loss as well as the associated costs of non-compliance, breach, and inappropriate or ineffective resource allocation. Moreover, such training can address the *human side* of electronic data security and privacy implementation, which the Expert Advisory Panel identified as a weak link.

Meaningful and instructionally sound training is critical to awareness and policy as it pertains to information management risk issues. Standardizing a high-level approach, performance objectives, instructional designs, and other components can ensure that states attend to the issues as they pertain to their unique circumstances and laws. Offering such training in the online environment eliminates the need for working around schedules and allows 24/7 access for "training on demand" without the traditional costs of training. It also makes it possible to control outcomes more closely and may be linked with self-assessments and online certificates of completion as well as leadership dashboard spaces, which can support decision-making.

Provide Guidance, Assistance and Incentives to States for Implementing Strong Authentication for Remote Access to Systems

We recommend that the Department provides guidance, assistance, and incentives to

states for implementing strong (i.e., two-factor) authentication, consisting of a password plus a PKI card; or a password plus a biometric, for remote access to systems. We recommend a data inventory of practices among other organizations, including Federal agencies, who are exploring this issue and developing adoption strategies.

Two-factor authentication as described is a recommended control for all Federal information systems in NIST Special Publication 800-53, Revision 3. Promoting this control can allow the Department to help states reduce the current risks of improper access via a compromised username/password combination.

There was some disagreement among the members of the Expert Advisory Panel regarding the feasibility of two-factor authentication at the school or district level, given the number of users possible in a given system. However, two-factor authentication is rapidly becoming the *de facto* standard for system access, and there are many implementation options.

Research

Conduct a Feasibility Study on Certifying Education Systems for Data Protection Security and Management

Related to the NIST recommendation above, we recommend that the Department investigate the feasibility of certifying education systems that meet an established level of data protection controls. Certification can ensure that systems meet a minimum and consistent baseline for data protection security and management. Systems could be categorized (in using a categorization analogous to the Federal Information Processing Standards (FIPS) 199) and tested at an appropriate risk level.

Certification can help support enforcement matters and address areas of concern that demand more attention.

Investigate Methods for Providing No-Cost or Low-Cost Security tools to Education Agencies

We recommend that the Department investigate alternative methods for providing no-cost or low-cost security tools to education agencies. While tools such as vulnerability scanning tools and intrusion detection systems can help mitigate risk in SLDSs, they can be costly to purchase. An investigation can be made to determine methods, such as discount programs for tools (such as Nessus®) or open-source based alternatives that can be offered to education agencies.

We recommend an analysis and breakdown of available tools so decision-makers can

have an opportunity to become familiar with the options and, subsequently make appropriate choices for their agency or school.

There was consensus among members of the Expert Advisory Panel that security tools and processes are a critical component of an overarching information management system. Not everyone agreed that cost-cutting should be a consideration; some felt that a low- or no-cost solution was appropriate given budgetary restraints.

Research and Report on Interagency Agreements

We recommend that the Department identifies, researches, and analyzes existing agreements between K-12 -higher education and other agencies; and, that it explores the conditions under which a state department of education might write an agreement with another state's department. For instance, the Department could research and analyze data-sharing with social services.

In this instance of investigating the linking of education and social services data, subtopics such as the following might be explored: 1) the impact of school mobility on student achievement for children and youth in foster care, and how it affects success in higher education and the workforce; 2) how services beyond the scope of the classroom (*e.g.*, health care, child welfare, higher education access and public safety) can be better tailored to help each student meet academic goals; 3) how initiatives aimed at improving child outcomes can be better aligned and coordinated among the education, child welfare and judicial systems to improve outcomes and reduce duplication; and, 4) what practices/programs have demonstrated the ability to improve outcomes for students, including not only educational achievement, but also social, health and civic progress. While this link is more likely to occur at the state level, some larger urban districts in which social service programs are offered may also benefit from sharing SLDS data with local social services departments.

Research and Report on Statistical Disclosure

We recommend attention to the topics of statistical disclosure and statistical disclosure limitation. Several members of the Expert Advisory Panel cited this area as a critical component of a well-constructed architecture.

Unintended disclosure of personal information can occur even in aggregated presentations of data. For instance, data on several state education web sites are presented in tables (giving e.g., student performance on assessments by grade and race) in ways that permit users to deduce the performance of individual students.

Unintended disclosure can also occur when data are reported as percentages rather than counts. Linkage to external databases using implicit identifiers (such as date of birth,

gender and residential zip code) can lead to re-identification of data records.

Research and Report on Student Unique Identifiers

We recommend that the Department consider a "top down" strategy to discourage the practice of allowing Social Security Numbers (SSNs) to be used as Sensitive Unclassified Information (SUI) at the state and district levels.

Some states are still allowing the use of SSNs as SUI. This raises significant privacy concerns as well as data security issue concerns. On May 22, 2007, the Office of Management and Budget (OMB) directed all Federal agencies to develop and implement a plan to eliminate the unnecessary use of SSNs.

Explore Unique Teacher Identifiers to Link Teacher and Student Data

We recommend that the Department explore the idea of unique teacher identifiers that could enhance connections between teacher training and qualifications and student academic performance and growth, in a privacy preserving form. Teacher identifiers could enhance the ability to match teachers to students by classroom and subject, a connection that is critical to understanding the relationship between teacher training and qualifications and student performance and academic growth. Collecting this data makes it possible to identify which students and which courses are being taught by teachers with different levels and types of preparation or certification, and which forms of teacher training and certification have the greatest impact on students' academic growth in the classroom.

With a teacher identifier and the ability to connect teacher and student data, policymakers and educators could have insight into: 1) the teacher preparation programs that produce graduates whose students have the strongest academic growth, 2) how the experience levels of the teachers in the district's high-poverty schools compare with those of teachers in the schools serving affluent students, and how these experience levels are related to the academic growth of the students in their classrooms, and 3) the relationship between the performance of the district's low-income students on the state algebra exam and teacher preparation in that subject.

National Conference of State Legislatures "State Security Breach Notification Laws." April 12, 2010. HYPERLINK "http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ SecurityBreachNotificationLaws/tabid/13489/Default.aspx"http://www.ncsl.org/IssuesResearch/ TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/ Default.aspx
 US-CERT, "Federal Incident Reporting Guidelines." HYPERLINK "http://www.us-cert.gov/federal/ reportingRequirements.html"http://www.us-cert.gov/federal/reportingRequirements.html
 National Institute of Standards and Technology and U.S. Department of Commerce, NIST Special Publication 800-53, Revision 3. HYPERLINK "http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/

sp800-53-rev3-final.pdf"http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

Emergency Management Institute Independent Study Courses. HYPERLINK "http://training.fema.gov/IS/searchIS.asp?keywords=PDS"http://training.fema.gov/IS/searchIS.asp?keywords=PDS

International Association of Privacy Professionals, "IAPP: International Association of Privacy Professionals." HYPERLINK "https://www.privacyassociation.org/"https://www.privacyassociation.org/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology "FIPS 199, Standards for Security Categorization of Federal Information and Information Systems." HYPERLINK "http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf"http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Tenable Network Security(R), "Tenable Network Security." HYPERLINK "http://www.nessus.org/nessus/"http://www.nessus.org/nessus/

OMB M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." HYPERLINK "http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf"http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf