Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

June 25, 2014

Media Contact: April Ward
(202) 226-8417

Statement of Subcommittee Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

"How Data Mining Threatens Student Privacy"

Remarks as Prepared

I would like to thank Ranking Member Clarke as well as Chairman Rokita and Ranking Member Loebsack from the Education and the Workforce Subcommittee on Early Childhood, Elementary, and Secondary Education for coming together with us to hold this joint hearing on a very important issue, the privacy and security of our students' personally identifiable information (PII). Today is marks the first joint hearing between these two committees, and I'm looking forward to working with Chairman Rokita and Ranking Member Loebsack on this issue.

In recent years the number of school districts using educational software and cloud services has greatly increased; today nearly 95% of school districts are using these services. These services can provide numerous advantages to school administrations and educators including individualized learning, state examination assessments and administrative functions such as attendance records. While these services can be helpful to our student's development, it is vitally important that we understand the privacy and security concerns of sharing such sensitive information. A report by the Fordham Law School found that cloud services used by school districts are poorly understood and have a lack of transparency, finding 20% of school districts do not have proper policies in place for the use of these services and fewer than 7% restrict the sale of student information by vendors.

Security of student information must be paramount, as this Subcommittee as examined in recent hearings cyber criminals have become more sophisticated in their tactics and techniques, evidenced by the increasing number of cyber breaches at universities, schools and retailers. The more interconnected our lives become with online services the greater the risk these criminals can exploit it. Over the past year three major universities and one school district have become victims of cyber breaches affecting hundreds of thousands of students' personally identifiable information.

Greater transparency is needed on behalf of the school districts and the vendors with which they contract. Parents enrolling their children in school should have a clear understanding of what information is collected, stored and shared. The Family Educational Rights and Privacy Act (FERPA) is the federal law that governs the privacy of student records. FERPA establishes when and what type of information school districts can share with private vendors. However, there are concerns that because FERPA was enacted in 1974, long before the advent of these technologies, it does not reflect the current reality in the classroom and the changes in how data is collected and shared.

Today's hearing will seek to examine the sharing of student information with educational software and cloud service vendors and the laws and guidelines that govern them. The Subcommittees will hear testimony from a distinguished panel including representatives from the Fordham Law School, Software and Information Industry Association, Idaho State Department of Education and the Alliance for Excellent Education. Transparency on behalf of the school districts and the educational companies is vitally important; parents should have a clear understanding of what schools are sharing and what rights they have. I appreciate the opportunity to work with my colleagues at Education and the Workforce to examine this important issue.

###