**Opening Statement**

**Rep. Gerald E. Connolly (VA-11)**

**Committee on Oversight and Government Reform**

**Hearing on the U.S. Department of Education: Information Security Review**

**Nov. 17, 2015**

Mr. Chairman, I appreciate the opportunity to examine the information technology and security programs and practices within the Department of Education and its Federal Student Aid program. The Department might not seem like an obvious target of cyber-related threats, but it is responsible for managing and securing a student loan portfolio of more than $1 trillion, along with the personal information of more than 50 million students between federal loan borrowers, Pell Grant recipients, and other assistance programs. **In the wake of the two massive data breaches disclosed by the Office of Personnel Management earlier this year – which collectively put at risk the personal information of more than 28 million current and former federal employees and their families, including Members of Congress like me – every federal agency ought to be reassessing its own information security protocols and reinforcing their efforts to detect and deter cyberattacks and other threats.**

Perhaps this should be the first of a recurring set of hearings to gauge successes and shortfalls across agencies when it comes to protecting the vast amount of sensitive information held by the federal government. I think we would find most agencies in a similar situation to the Department of Education, which has made some progress in fortifying its information security defenses in recent years yet continues to struggle with recurring vulnerabilities. In its latest report on the Department’s efforts to implement the Federal Information Security Modernization Act (or FISMA), the Inspector General identified 16 findings with 26 recommendations, one-third of which are repeat recommendations. Last year’s audit “found that the Department did not perform adequate remediation of weaknesses identified in previous OIG audit reports.” **While it appears the Department has beefed up its remediation efforts, there still is much work to be done, and I am confident this is not the only Department with these challenges.**

This year’s audit flagged weaknesses across four key areas: continuous monitoring, configuration management, incident response and reporting, and remote access management. For example, the IG found user accounts, from inside federal employees and outside federal contractors, with excessive or unnecessary permissions and unauthorized access to data. In fact, one of the Department’s  IT service contractors could not verify to the IG’s satisfaction that its other, non-federal customers did not have unauthorized access to the Department’s data through a shared service. Even more troubling, the OIG said it was able to not only gain access to the Department’s network through a simulated attack, but also launch other attacks on systems connected to the Department while going completely undetected.

Another critical finding in the IG’s report that applies to the Department of Education, as well as all federal agencies, is that existing information security protocols if implemented, and implemented consistently throughout the organization, should be effective. Nowhere is this more important than in cyber security and privacy training for new employees. To be successful here, we must bring about a wholesale cultural revolution so that federal agencies and the workforce understand the critical importance of cyber safety, including basic elements of what many call “cyber hygiene.” Along those same lines, we must hold agencies accountable for implementation of the bipartisan Federal IT Acquisition Reform Act (FITARA), on which we recently held a hearing and issued a preliminary scorecard for agency progress. One of the key reforms of that legislation, which I was pleased to co-author with the former chairman of this committee, is enhancing CIO authorities to increase transparency and improve risk management to address these very issues.

**The severity of recent data breaches in both the public and private sectors in recent years underscores the urgency for federal agencies and Congress to get serious about investing in IT solutions that better secure our data and taking actions that will be a deterrent for hackers.** This is a challenge that has confounded both Democratic and Republican Administrations. The number of IT security incidents reported by federal agencies increased from 5,503 in 2006 to 67,168 in 2014 -- an increase of 1,121 percent!

Unfortunately, these attacks on our private industries and government simply reflect the new normal of the 21st Century, where nation-states represent advanced and persistent threats against one another, constantly seeking to gain unauthorized access to sensitive and classified information on each other’s people, intellectual property, and sensitive security information. **The likes of North Korea, China, Russia, and Iran are increasingly testing the waters and becoming emboldened by a lack of reprisal or deterrence.**

The House earlier this year did pass two bills on a bipartisan basis to encourage voluntary sharing of information between the public and private sectors, but information sharing alone is not enough. We need to get serious about strengthening our cyber workforce, both within the federal government and among our private sector partners. We also need to devise more effective data breach notification policies. As my colleagues know, it’s now been almost four months since the breach on background records was announced and notifications are still being made.

So, Mr. Chairman, I appreciate this opportunity to look at what the Department of Education is doing right, and what it can improve upon, with respect to securing its data, but it cannot be the only one. **Successfully detecting, defending, and deterring cyber threats, will take a concerted effort across all agencies and among our private partners.**