COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Oversight Subcommittee Chairman Barry Loudermilk (R-Ga.)
Cybersecurity: What the Federal Government Can Learn from the Private Sector

Chairman Loudermilk: Thank you, Chairwoman Comstock, for continuing this very important discussion on the security of our federal information systems. I would like to thank our witnesses for being here today to help us understand industry's best practices when it comes to cybersecurity. I look forward to hearing about lessons learned and how to apply those lessons to our federal systems to help prevent future cyber attacks.

It is clear that our federal systems are not adequately protected. In fact, just this past summer, a witness from the Government Accountability Office (GAO) before this Committee stated, "…it's incumbent upon federal agencies to implement the appropriate security controls to mitigate those risks at a cost-effective and acceptable level. And, we found that agencies have not consistently implemented agency-wide information security programs to mitigate that risk effectively." When I asked that same witness to grade our federal cybersecurity, he gave it a D.

A rating of D is not an acceptable grade. This Administration owes it to the American people to significantly improve this deplorable standing in order to sufficiently protect government information and thereby our national security. This Administration also needs to explain how it is protecting the American people's personal information.

As I stated at the aforementioned hearing this summer, the breach of data from the Office of Personnel Management (OPM) is exactly why the Oversight Subcommittee that I Chair continues to look into the collection of Americans' personal data through the website HealthCare.gov. In fact, I am still waiting for complete answers from the Administration to questions I posed in letters to the Office of Science and Technology Policy (OSTP) and the Centers for Medicare and Medicaid Services (CMS) in June.

This Administration has not sufficiently explained why it was ever necessary to indefinitely store Americans' personal data they submitted when logging into the HealthCare.gov website – particularly those who did not end up enrolling. One would think that President Obama would agree that such a practice to be unnecessary as he "identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter." If cybersecurity is one of the most serious

challenges that this government faces, why on earth would the government ever consider storing all of this personal information – indefinitely - in a data warehouse?

As the Chairman of the Oversight Subcommittee, I will continue to ask questions and demand answers until we are satisfied that federal departments and agencies are making decisions in the best interest of protecting the personal information of all Americans. The safety and security of Americans and this nation must be our number one priority. Having continuous, subpar security of our federal systems is embarrassing and must be rectified immediately. The delays must stop. It is time to finally do something about federal cybersecurity.

I look forward to the witnesses' testimony at today's hearing. I hope to learn more about the various industry best practices and lessons learned in hopes that it will shed a light on what the government could and should be doing to protect our citizens from constantly evolving cyber threats.

###