COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
CHAIRMAN LAMAR SMITH

For Immediate Release
July 8, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Oversight Subcommittee Chairman Barry Loudermilk (R-Ga.)
Is the OPM Data Breach the Tip of the Iceberg?

Chairman Loudermilk: Thank you, Chairwoman Comstock, for holding this very important hearing on an issue that hits too close to home for you as well as many others in this country. I would like to thank our witnesses for being here today in order to help us understand what seems to be an epidemic of cyber-attacks. I look forward to discussing what needs to be done to prevent similar attacks from occurring in the future.

Unfortunately, this Administration has failed to provide Americans with any level of confidence that it will adequately protect their personal information when entrusted with it. As we have witnessed over the past few months, there has been a concerning pattern of security breaches involving government computer systems. This includes the recent, massive data breach of the Office of Personnel Management (OPM) -- disclosing personal and official information that could potentially harm our national security. For an Administration that touts that it has "prioritized the cybersecurity of federal departments and agencies," we have instead witnessed a government that is unable to properly secure its computer systems and protect sensitive information.

The situation at OPM is exactly why the Subcommittee that I Chair is looking into the collection of Americans' personal data through the HealthCare.gov website. In that situation, it appears that social security numbers, dates of birth, names, mailing addresses, phone numbers, financial accounts information, military status, employment status, passport numbers, and taxpayer IDs are being retained. This information is being stored in a "data warehouse that is intended to provide reporting and performance metrics related to the Federally Facilitated Marketplace (FFM) and other Healthcare.gov-related systems."

In the situation of the data warehouse, the Administration never appeared to be forthright about the use and storage of personally identifiable information on HealthCare.gov. The Administration has yet to explain the reason for indefinitely storing user information, particularly of the users of the website who input their data to log in, but do not end up enrolling.

If that data warehouse is being protected in the same way that OPM was protecting personal information, action needs to be taken now to avoid putting the American people at significant personal risk. With many Americans being forced into the government health care exchange, a breach of this system could end up having millions affected, just like the OPM data hack.

The Government Accountability Office (GAO) has included the cybersecurity of federal information systems on its list of high risk areas since 1997, so this isn't something new. Why, then, are we sitting here almost twenty years later, wondering why our federal information systems are not being adequately secured? In the most recent GAO High Risk Series report, it says that "…inspectors general at 22 of the

24 agencies cited information security as a major management challenge for their agency. For fiscal year 2014, most of the agencies had information security weaknesses in the majority of five key control categories."

As the Chairman of this Committee's Oversight Subcommittee, I want to find the truth behind this reckless behavior that is threatening the safety and security of the American people. These actions – or rather, lack of actions - put the future of our nation at great risk, and must stop.

I look forward to today's hearing, which I anticipate will inform us more about the recent OPM breach and the current state of our federal information systems. We owe it to the American people to ensure that their personally identifiable information is safe and protected from cybercriminals.

###