COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
CHAIRMAN LAMAR SMITH

For Immediate Release
July 8, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Research & Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)
Is the OPM Data Breach the Tip of the Iceberg?

Chairwoman Comstock: Just over a month ago the Office of Personnel Management (OPM) announced a massive data breach that exposed the personal information of over 4 million current and former federal employees and contractors.

Like thousands of my fellow constituents, I received a letter from OPM informing me that my personal information may have been compromised or stolen by the criminals behind this attack.

Unfortunately, the news gets worse this week, as we learn more about the reported second OPM data breach, compromising the security of 18 million federal employees, contractors and others who submitted sensitive information for background checks. And sadly the response from OPM has not inspired confidence.

Identity theft by what seems to be a foreign entity is a very serious national security issue. They are at cyberwar with us – do our leaders appreciate that reality?

Many of my constituents have contacted me about their fears and concerns. It has been months since OPM discovered the attack, and we still have too many questions and not enough answers.

As we will hear from witnesses today, Federal employees have many unanswered questions. Just one: Are the credit monitoring identity theft provisions adequate? Most alarming to me about these breaches is that they were launched less than 18 months after a previous severe network assault on OPM. We know that information security incidents reporting by federal agencies has increased by 1000 percent since 2006.

For years the OPM Office of Inspector General and the U.S. Government Accountability Office have been warning OPM leadership of critical vulnerabilities to their information systems. Some of the weakness and current problems were ID'd as far back as 2007. Today, many of their recommendations for fixing the systematic failures remain unmet.

Cyber criminals and foreign enemies are working night and day with the latest technology to exploit every vulnerability in our system, while OPM is behind the times and operating apparently at a pace with systems designed for the last century not for the current threat. The United States has some of the world's best technological minds and resources, yet OPM's management is failing.

Federal employees provide their sensitive personal information under the expectation that it is protected with all due seriousness. However, the trust between our federal employees, contractors, and others whose information has been compromised is damaged.

Cybersecurity must be a top priority in every government agency from the top Cabinet official on down. We need an aggressive, nimble, and flexible strategy to anticipate, intercept, and stop cyberattacks. Those who are engaging in cyberattacks on our citizens, agencies, and companies – whether they be nation states, adversaries or hacktivists – are a reality we will be living with in the 21st century and we must develop and use all the tools and technology available to thwart them and understand this is an ongoing problem we have to constantly be on top of.

I want to note that we invited the OPM Chief Information Officer Donna Seymour to testify at today's hearing. She declined the Committee's invitation, citing other commitments, we continue to have questions about how and why this cyberattack occurred and the measures that have been instituted to prevent a future attack at OPM. We will take any necessary steps to ensure my constituents get those answers.

Today's panel of witnesses will help us better understand the magnitude of cybersecurity challenges at OPM and across the federal government, as well as determine what steps need to be taken to prevent future cyberattacks, and the state of the art best practices to do so.

I appreciate the leadership of Chairman Lamar Smith on these issues and the role the Science Committee has played in making cybersecurity R&D a priority.

I look forward to continuing to lead the Research & Technology Subcommittee in efforts to make sure the federal government is staying ahead of our adversaries who are constantly developing new and sophisticated malicious technologies.

If officials neglected their duties, or are not the right people for the job, they must be held accountable so that proper leadership is in place to not just meet, but anticipate and beat the next cyber threat.

###