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

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Research and Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Chairwoman Comstock: Today's hearing continues this Committee's commitment to find solutions for one of the great challenges of the 21st Century – cybersecurity.

This is the second hearing we have held on cybersecurity since the news over the summer that the Office of Personnel Management (OPM) was the target of two massive data breaches – exposing the sensitive information of over 21.5 million Americans, including many of my constituents.

The OPM breach highlighted the growing challenge of preventing and responding to cyber threats for both the public and private sectors.

In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, and Anthem Health Insurance were only a few of the many publicly disclosed breaches. The data breach of Anthem alone exposed the social security numbers of 80 million Americans.

The time has come for every manager and every employee in both government and private organizations to make cybersecurity a top priority in their daily work, and for leaders to be held accountable for negligent failures to protect information.

The American public and shareholders are demanding it. When criminal hackers gained access to some 40 million Target customer credit cards, the CEO and CIO were fired.

Although the OPM Director resigned in the wake of the OPM breaches, I am still not satisfied that the responsible parties have been held accountable for the failure of the agency to address known security vulnerabilities.

The most recent IG audit found that OPM still has 23 systems that have not been subject to a thorough security controls assessment. OPM does not even have a complete inventory of servers, databases and network devices in their system.

Just this week I met with newly appointed Senior Cyber and Information Technology Advisor Clifton Triplett and the OMB Senior Advisor on Cyber and National Security. I

look forward to working with my colleagues and all federal agencies to ensure we are protecting the identities of our employees, applicants, and their families.
The cyber criminals, "hacktivists", and state- sponsored cyber terrorists are getting more creative and bolder in their attacks.

The private sector has been at the forefront of dealing with these threats for some time, as both the target of many of these attacks and as the leaders in developing the technology and workforce necessary to counter cyber threats.

Visa, a global payment company, is preparing to open a new Cyber Fusion Center in my district just next week. This state of the art cyber facility brings together nearly 100 highly trained security professionals into one high-tech campus, and provides for collaboration both internally and with payments ecosystem partners -enabling information sharing, rapid response, coordinated command and control for defensive operations, and launching a real-time visualization of security events & response.

I look forward to hearing from our witnesses today, who are all innovative thinkers from the private sector. I hope we can take the lessons we learn from you today, and help apply them towards protecting our federal information systems and the sensitive and valuable information they contain.

Leaders in government and the private sector must work together to create a culture that ensures everyone considers cybersecurity a shared responsibility.

###