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

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)

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

Chairman Smith: Thank you Madam Chair, I look forward to today's hearing. Our witnesses' expertise and experience with cyber threats in the private sector will enable us to improve the federal government's response to cyber-attacks.

Last year, more than 178 million records of Americans were exposed in cyber-attacks. The breach of the Office of Personnel Management (OPM) alone compromised the personal information of more than 20 million people, which included Members and staff of this Committee.

The United States is a top target by foreign countries. Cyber criminals and "hacktivists" exploit vulnerabilities in our networks and cyber-systems to obtain valuable information.

The number of cybersecurity incidents reported by federal agencies has increased over 1,000 percent in the last eight years. In 2014, more than 67,000 cyber-attacks were reported. Many others were not.

A number of federal agencies guard America's cybersecurity interests. Several are under the jurisdiction of the Science Committee. These include the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Homeland Security's Science and Technology Directorate, and the Department of Energy.

All of these agencies support critical research and development to promote cybersecurity and set federal standards. However, it is clear that too many federal agencies, like OPM, fail to meet the basic standards of information security. More must be done to ensure agencies make cybersecurity a top priority.

Last year, audits revealed that 19 of 24 major federal agencies failed to meet the basic cybersecurity standards mandated by law. Yet the administration has allowed deficient systems to stay online.

What are the consequences when a federal agency fails to meet its basic duties to protect sensitive information?

What does it say to federal employees, not to mention our adversaries, when cabinet secretaries don't take cybersecurity seriously and fail to follow the most basic e-mail security practices involving our country's classified information?

In the private sector, those who neglect their duty to keep the information of their customers secure are usually fired. In the federal government, it seems the only people penalized are the millions of innocent Americans who have their personal information exposed.

During the last Congress, the Science Committee approved the *Cybersecurity Enhancement Act*, which was signed into law. This law improves America's cybersecurity abilities and strengthens strategic planning for federal cybersecurity research and development. It supports NSF scholarships to improve the quality of our cybersecurity workforce. It also improves cybersecurity research, development and public outreach organized by NIST.

Last month, a similar bill, the *Cybersecurity Act of 2015*, was signed into law. Very importantly, this bill encourages private companies to voluntarily share information about eminent cyber threats with each other as well as with the federal government.

The Science Committee will continue its efforts to support research and development to strengthen America's cyber defenses.

I look forward to hearing from our witnesses today about what more we can do to support innovation and help set national standards and guidelines that will enhance our country's cybersecurity.

###