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

For Immediate Release
October 21, 2015

Media Contact: Laura Crist
(202) 225-6371

Statement of Subcommittee on Research & Technology Chairwoman Barbara Comstock (R-Va.)
Cybersecurity for Power Systems

Chairwoman Comstock: Within the past few years, we have seen a significant increase in cybersecurity attacks affecting a wide-array of sectors. These attacks have exposed the personal information of millions of Americans, highlighting a very serious national security issue.

Specifically, in the recent breach of the Office of Personnel Management, identity and financial information was stolen by what is suspected to be a foreign source. This breach compromised the information of more than 21 million individuals' financial and personal information, including tens of thousands in my district as well as my own information.

As the electric power industry modernizes to a more interconnected smart grid, the threat of a cybersecurity breach significantly increases in that sector. Fortunately, while we have yet to see a successful cyber attack to our nation's electric grid, USA Today found that the United States' power grid "faces physical or online attacks approximately 'once every four days.'"

In addition, in 2014, the National Security Agency (NSA) reported that it had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems, and other critical infrastructure."

Although we have not seen any significant operational impact on the grid, this unfortunately does not mean that we are completely protected. In fact, it is believed that adversaries have been able to get into and observe our control systems in order to prepare for a potential future attack.
In addition, over the summer, FBI Director James Comey said that his agency had picked up signs of terrorist groups having increased interest in cyberattacks.

Because of these constant threats, we need to ensure that the techniques and technologies in place today can prevent adversaries from obtaining access to our systems and can continue to prevent cyber attacks from disrupting our national power supply.

The National Institute of Standards and Technology (NIST) plays a large role in this as it works with stakeholders and partners from industry, government, and academia to build a framework and roadmap for smart grid interoperability standards to ensure that all of the many pieces of the smart grid are able to work together.

Further, NIST formed a Smart Grid Interoperability Panel Cybersecurity Committee to address and advance the development and standardization of cybersecurity. The Committee's objective was to advance the development and standardization of cybersecurity, including privacy, policies, measures, procedures, and resiliency in the electric smart grid. Just last year, NIST published its Framework and

Roadmap for Smart Grid Interoperability Standards, Release 3.0, around the same time that it made revisions to its guidelines for smart grid cybersecurity.

I am interested in learning about how the NIST guidelines for smart grid cybersecurity are implemented in government and industry and how they contribute to a more resilient grid. In addition, I am looking forward to hearing about the technologies and techniques that are being developed and used in order to protect our nation from a massive attack to our control systems.

As someone who was personally affected by the OPM breach, which occurred despite years of warnings from the OPM Office of Inspector General and the U.S. Government Accountability Office to OPM leadership about critical vulnerabilities to their information systems, I know firsthand that we cannot ignore any kind of cybersecurity threats and vulnerabilities.

The fact that we know of adversaries who have been able to get into and observe our systems highlights the need to be proactive in protecting our grid to prevent such bad actors from being capable of taking down our control systems.

I look forward to today's hearing and thank our witnesses for being here. It is clear that there are many threats to our critical infrastructure, and we must ensure that our federal systems are adequately protected, especially as we transition to the Smart Grid.

Continuing to evolve our technologies and standards in order to mitigate these vulnerabilities and their potential consequences is ultimately essential for the safety and security of all Americans.