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

For Immediate Release
October 21, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)
Cybersecurity for Power Systems

Chairman Smith: Good morning. Today we will examine the ongoing efforts by federal agencies, the Department of Energy national labs and the private sector to protect Americans from cybersecurity threats to our power supply.

This hearing also will explore solutions to combat the cyber threats identified in a Science Committee hearing held last month, which focused on the broader vulnerabilities of the American power supply. Cyber-attacks are a threat to our country and our citizens. Many Americans think the primary risks from cyber-attacks are only attempts to steal information, such as with the Office of Personnel Management attack earlier this year.

However, the threat to America's power supply from these attacks increases every day. As we will hear from one of today's witnesses, a compromised electric grid is not a question of "if" but "when."

As cyber attackers become more sophisticated, it becomes more difficult for those who are vulnerable to protect themselves. Electric utilities must operate complex systems of power plants, transmission lines and distribution facilities, all interconnected through analogue and digital control systems.

Each system connection creates an area of vulnerability, which requires real-time monitoring and the ability to respond to incoming threats throughout the energy system. And as power plant systems are modernized and diversified, two-way digital communication adds even more risk.

But the current system of federal cybersecurity mitigation is fragmented and complex.

Cybersecurity standards, research and development are conducted at the Department of Homeland Security, the Federal Energy Regulatory Commission, the Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability, the National Institute of Standards and Technology (NIST), and the DOE national labs.

Each federal entity conducts an important role, which ranges from the development of guidelines for critical infrastructure operators to ways to provide risk assessment modeling and control system testing. The development of effective cybersecurity technology will require cooperation across federal agencies and the coordination of basic science and engineering research and development programs.

This level of cooperation is a challenge to accomplish across government agencies. And when we factor in the private sector's unique role it becomes even more complex.

Agencies will need to think creatively and work together to simplify the information-sharing process for industry.

If the system of federal guidelines and regulations is too complex, industry will not be able to effectively use monitoring and information-sharing networks established by federal agencies. The Department of Energy, NIST, and the Department of Homeland Security cannot effectively protect the electric grid without interagency cooperation.

I thank our witnesses today for their efforts to protect our critical infrastructure. I look forward to hearing how federal agencies can work with industry to secure the electric grid and what role Congress should play in the direction and oversight of this complex process.

Affordable, reliable power is the foundation of the American economy. Federal research and development that leads to ways to secure our power supply from cyber-attacks should be a priority, particularly through cooperation between the national labs and industry.

We must develop smart technology that can protect consumer data and keep our electric grid secure.