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

For Immediate Release
October 21, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Energy Subcommittee Chairman Randy Weber (R-Texas)
Cybersecurity for Power Systems

Chairman Weber: Good morning and welcome to today's joint Energy and Research and Technology Subcommittee hearing examining cyber threats to American energy systems. Today, we will hear from an expert panel on the growing threat of cyber-attacks to the nation's electric grid.

Our witnesses today will also provide insight into how industry and the federal government are working together to anticipate cyber threats, and improve the reliability and resiliency of our electric grid against cyber-attacks.

The reliability of America's power grid is one of our greatest economic strengths. In my home state of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 people per day, and provides power to the energy intensive industries that drive consumption. Texas is by far the nation's largest consumer of electricity. Keeping the Texas power grid reliable and secure is key to continuing this economic growth.

But as we established in a hearing on broad threats to the power supply earlier this year, utilities face significant threats to the reliability of power delivery. Our electric grid is particularly vulnerable to growing cybersecurity threats as the grid is modernized, as distributed energy, electric vehicles, and modernized digital operating systems create more access points for cyber-attacks.

And while the nation's industrial control systems for the grid are analogue systems designed to last for decades, digital IT systems must constantly adapt to combat evolving cyber threats.

Small scale cyber and physical attacks to our electric grid are estimated to occur once every four days. And in over 300 cases of significant cyber and physical attacks since 2011, suspects have never been identified.

We often think of cybersecurity and other threats to the power grid at a macro scale, but these types of attacks can occur even at the local level. In 2011, the Pedernales Electric Co-op, a non-profit co-op that serves approximately 200,000 customers north of San Antonio, was struck by a cyberattack. While the attack thankfully did not disrupt power to consumers, it is a stark reminder that threats to the grid are real, and are not going away.

Our nation's power supply cannot be protected overnight, particularly as utilities struggle to adapt technology to manage a growing number of cybersecurity threats. Cyber threats to the power grid will continue to evolve, particularly as more interconnected smart technologies are incorporated into the electric grid.

And as protective technology improves, so does the capability and creativity of those conducting attacks.

While we cannot predict every method of attack, the federal government can and should play a role in assisting industry with developing new technology and security safeguards.

Accordingly, research and development efforts at the Department of Energy are focused on providing industry with comprehensive tools to conduct internal analysis to identify and address cybersecurity weaknesses so that industry can take the lead in addressing these vulnerabilities.

That's why testing facilities and cooperative research, like the Cyber Security Test Bed at Idaho National Lab, are valuable tools to combat cyber threats. At INL, industry can test control systems technology in real world conditions, reducing response time and risk for future attacks.

I want to thank our witnesses for testifying before the Committee today. I look forward to a discussion about cyber threats to our critical infrastructure, and how the federal government can provide industry with the tools and technology necessary to fight the next generation of cyber-attacks.