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

For Immediate Release
September 10, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Energy Subcommittee Chairman Randy Weber (R-Texas)
Examining Vulnerabilities of America's Power Supply

Chairman Weber: Good morning and welcome to today's joint Oversight and Energy Subcommittee hearing examining vulnerabilities of America's power supply. Today, we will hear from a broad range of witnesses on the existing threats to the nation's electric grid, and the impact that potential attacks and incidents could have on our grid reliability and national security.

Our witnesses today will also provide insight into how industry and the federal government can work together to harden our electric grid against ongoing and changing threats.

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 it is common knowledge that utilities face significant and diverse threats to the reliability of power delivery. Our electric grid is vulnerable to physical threats caused by damage to existing infrastructure and growing cybersecurity threats as the grid is modernized.

Key infrastructure such as utility substations are often left completely exposed, with little more than a chain-link fence protecting the facilities that keep the lights on across the country. 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.

Our power grid is also at risk from geomagnetic disturbances, which can be caused by space weather or an Electromagnetic Pulse, commonly known as E-M-P, which could be generated in a nuclear attack. These high energy pulses could severely impact the operation of the electric grid and electric power systems across the country, disabling and damaging equipment essential to providing reliable power that could be nearly impossible to replace on a large scale.

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 electric reliability, 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. 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.
I want to thank our witnesses for testifying before the Committee today, and I look forward to a discussion about the threats to America's reliable power supply and the federal government's role in helping to secure our electric grid.

###