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

For Immediate Release
September 10, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Oversight Subcommittee Chairman Barry Loudermilk (R-Ga.)
Examining Vulnerabilities of America's Power Supply

Chairman Loudermilk: Good morning. I would like to thank our witnesses for being here today to help us examine the vulnerabilities of America's power supply.

The electricity infrastructure of the United States is aging, and the electric power industry is in the process of modernizing it with its transformation to the "smart grid" -- the technology that provides an increased use of digital information and control technology to improve reliability, security, and efficiency of the electric grid.

That process of modernization, however, introduces new vulnerabilities in addition to ones that have existed for over a century. This hearing will discuss those various threats to the national electric grid, including: severe weather or other natural events; cyber, physical, or coordinated attacks; space weather; and electromagnetic pulse (EMP) attacks.

The blackout that darkened the Northeast in the summer of 2003 opened many eyes to the vulnerability and age of our electrical system. In that case, a tree branch in Ohio coupled with software issues and human error left many in the dark for two days. In addition to natural events like this and Superstorm Sandy - which left millions of people without power, man-made physical threats exist.

In 2013, unknown attackers coordinated an attack on a Pacific Gas & Electric Metcalf substation in California. Those attackers severed six underground fiber optic lines and fired over 100 rounds of ammunition at transformers. While the attack did not lead to any loss of power or life, it caused over $15 million in damage. The President and CEO of the American Public Power Association stated at a hearing last year that, "shooting at substations, unfortunately, is not uncommon."

Just as troubling is the amount of attempted cyber-attacks to the nation's electric grid. An investigation completed by USA Today earlier this year 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." We have also been examining cyber threats in the Homeland Security Committee, and this is an absolutely critical issue that must be taken seriously by Congress and the entire federal government.

On top of these threats, we also have the potential threat of an electromagnetic pulse, which would disrupt or destroy electronic equipment after the detonation of a nuclear weapon. Geomagnetic disturbances can also be brought on by naturally occurring solar weather events, such as in 1989 when a geomagnetic disturbance caused millions of Canadians to lose their power for about nine hours.

It is clear that there are many threats to our electric infrastructure, and we must therefore ensure that our federal systems are adequately protected, especially as we transition to the "smart grid." We need to rethink how we protect our facilities from physical attacks, like the Metcalf incident where investigators were never even able to identify the criminals.

In addition, as we have seen over the past few years, cybersecurity is an ever-evolving threat. The fact that we know of intrusions by entities with the capability to take down our control systems means that we must do everything in our power to be proactive rather than reactive in order to protect our grid and prevent such a take-down from happening.

Mitigating these vulnerabilities and their potential consequences is ultimately essential for the safety and security of all Americans. Protecting our power supply is something that is crucial for day to day life activities and things that we take for granted – like heating and cooling a home or powering a business – as well as ensuring our national security.

I look forward to today's hearing, where I hope to learn more about the various vulnerabilities of our grid as well as the extent of the threats that could potentially leave us in the dark.

Thank you.

###