Opening Statement of the Honorable Ed Whitfield
Chairman, Subcommittee on Energy and Power
Committee on Energy and Commerce
Hearing entitled "Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act"
May 31, 2011

Today's hearing focuses on a critical national security issue – protecting the nation's electric grid from physical and cybersecurity threats and vulnerabilities.

A secure grid is of utmost importance to our national security and our national economic interests. The grid is vital to all aspects of American life. The daily lives of all Americans are powered by electricity provided by the electric grid, the disruption of which would cut off the supply of electric power to our homes, hospitals, schools, offices, farms and factories.

Cybersecurity threats and vulnerabilities to the electric grid have increased in recent years and were the subject of several hearings in the 110th and 111th Congresses. There is evidence that 'bad actors' have conducted cyber 'probes' of U.S. grid systems, and that cyber attacks have been conducted against critical electric infrastructure in other countries.

This past February, a cyber attack dubbed "Night Dragon," which is believed to have emanated from China, targeted the critical infrastructure of energy and petrochemical companies. The Night Dragon attack was not overly sophisticated, but was nevertheless successful in breaching the computer systems of key assets.

This example is one of several, and is the tip of the iceberg, and illustrates that we must be more vigilant in securing the nation's critical energy infrastructure, including the electric grid.

Beyond potential cyber attacks, the bulk power system remains exposed to physical vulnerabilities and threats, including direct terrorist attacks, weapons that can create an electromagnetic pulse, and geomagnetic storms.

Federal and state agencies and industry stakeholders have sought to address many of these concerns. In particular, through an extensive stakeholder process, the North American Electric Reliability Corporation (NERC), pursuant to its authority under Section 215 of the Federal Power Act, has worked over the last several years to develop and implement reliability standards and cybersecurity infrastructure protection standards.

Many believe, however, that the NERC process could be improved for responding to imminent threats and to address grid security vulnerabilities in a timely manner.

To address these shortcomings, the Committee recently released a discussion draft entitled the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act." The bill is identical to bipartisan legislation developed by this Committee last Congress by Chairman Upton and Mr. Markey.

The GRID Act arms the Federal Energy Regulatory Commission (FERC) with emergency authority to respond to imminent physical and cyber threats to the bulk power system and electric infrastructure that serves facilities vital to our national defense. This emergency authority can be triggered only upon a directive from the President.

The discussion draft also provides FERC with authority to identify and remedy weaknesses that leave the grid vulnerable to cyber attacks and electromagnetic pulse events.

Notably, the legislation also directs FERC to develop regulations to facilitate the sharing of information, as appropriate, between governmental agencies, NERC, and owners and operators of the bulk power system. Doing so will improve communication among affected stakeholders, which will result in a more secure grid.

Although the discussion draft is identical to last year's bill, we expect that input and insight provided by today's witnesses will help us improve the bill to reflect current conditions and any changed circumstances.

I thank the witnesses for being here today and look forward to the discussion.

With that I yield to the Ranking Member, Mr. Rush.