Mr. Chairman, Ranking Member and members of the Committee: Thank you for the privilege to appear before you today to discuss the security of the electric grid. My name is Joe McClelland and I am the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. I am here today as a Commission staff witness, and my remarks do not necessarily represent the views of the Chairman or any individual Commissioner.

The Commission is committed to protecting the reliability of the nation's bulk power system. Nevertheless, limitations in federal authority do not fully protect the grid against physical and cyber threats. My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act, and the Commission's implementation of that authority with respect to cyber-related reliability issues, primary through Order 706.

In the Energy Policy Act of 2005, Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability and cyber security standards for the nation's bulk power system. This authority is in new section 215 of the Federal Power Act.

Under the new authority, FERC cannot author or modify reliability standards but must select an Electric Reliability Organization, or ERO, to perform this task. The ERO develops and proposes reliability standards or modifications for the Commission's review, which it can then either approve or remand.

If the Commission approves the proposed reliability standard, it applies to the users, owners and operators of the bulk power system, and becomes mandatory in the United States. If the Commission remands a proposed standard, it is sent back to the ERO for further consideration.

The Commission selected the North American Electric Reliability Corporation, or NERC, as the ERO. It is important to note that FERC's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, which excludes Alaska and Hawaii, distribution systems, and can exclude transmission facilities in certain large cities, such as New York.

In addition to the reliability authority, FERC is also charged with oversight of the cyber security of the bulk power system. As is the case with non-security issues, FERC's authority under 215 over cyber security is exercised through the reliability standards developed by the ERO and approved by FERC.

Pursuant to this duty, FERC approved eight cyber security standards known as the Critical Infrastructure Protection standards, or CIP standards, proposed by NERC, while concurrently directing modifications to them in January 2008. Three sets of modifications responding to the Commission's directives have been received from the ERO, and the last was approved earlier this year. Although the CIP standards are approved, full compliance with these standards will not be mandatory until 2014.

More importantly, in approving the latest revision of the CIP standards, the Commission recognized that they are an interim step and raised its concern that the newly revised standards do not provide enough protection to satisfy the Commission's January 2008 order. Thus, the Commission established a deadline of the first quarter of 2013 for NERC to file standards in compliance with the outstanding directives in that order.

Physical attacks against the power grid can cause equal or greater destruction than cyber attacks. One example of a physical threat is an electromagnetic pulse, or EMP, event. In 2001, Congress established a commission to assess the threat from EMP.

In 2004 and again in 2008, the commission issued its reports. Among the findings in the reports was that a single EMP attack could seriously degrade or shut down a large part of the electric power grid. Depending upon the attack, significant parts of the electric infrastructure could be, quote, "out of service for periods measured in months to year or more."

In addition to man-made attacks, EMP events are also naturally generated, caused by solar flares and storms disrupting the earth's magnetic field. Such events can be powerful and can also cause significant and prolonged disruptions to the power grid.

The standards development system utilized under FPA 215 develops mandatory reliability standards using an open and inclusive process based on consensus. Although it can be an effective mechanism dealing with the routine requirements of the power grid, it is inadequate when addressing threats to the power grid that endanger national security.

Despite its active role in approving reliability standards, FERC's current legal authority is insufficient to assure direct, timely and mandatory action to protect the grid, particularly where certain information should not be publicly disclosed.

Any new legislation should address several key concerns. First, legislation should allow the federal government to take action before a cyber or physical national security incident has occurred. Second, any legislation should ensure appropriate confidentiality of the sensitive information submitted, developed or issued under this authority. Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize federal action to mitigate cyber or other national security threats to reliability that involve certain critical facilities in major population areas.

Finally, it is important that entities be able to recover costs that they incur to mitigate vulnerabilities and threats.

Thank you for your attention today, and I am available to address any questions that you may have.