Summary of Testimony of The Honorable Joseph T. Kelliher
Chairman of the Federal Energy Regulatory Commission
Before the Subcommittee on Energy and Air Quality
Committee on Energy and Commerce
United States House of Representatives
September 11, 2008

"Protecting the Electric Grid from Cyber Security Threats"

The Energy Policy Act of 2005 (EPAct 2005) authorized the Federal Energy Regulatory Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the bulk power system. These reliability standards are proposed to the Commission by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC), after an open and inclusive stakeholder process. The Commission cannot author the standards or make any modifications, and instead must either approve the proposed standards or remand them to NERC. FERC is well underway in implementing the new law, including now having in place an initial set of cyber security standards, for which full compliance is not required until 2010.

Section 215 is an adequate statutory foundation to protect the bulk power system against most reliability threats. However, the threat of cyber attacks or other intentional malicious acts against the electric grid is different. These are national security threats that may be posed by foreign nations or others intent on attacking the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance.

Damage from cyber attacks could be enormous. A coordinated attack could affect the electrical grid to a greater extent than the August 2003 blackout and cause much more extensive damage. Cyber attacks can physically damage the generating facilities and other equipment such that restoration of power takes weeks or longer, instead of a few hours or days. Widespread disruption of electric service can quickly undermine our government, military readiness and economy, and endanger the health and safety of millions of citizens. Thus, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect security-sensitive information from public disclosure.

The Commission's legal authority is inadequate for such action. This is true of both cyber and non-cyber threats that pose national security concerns. In the case of such threats to the electric system, the Commission does not have sufficient authority to timely protect the reliability of the system. Legislation should be enacted allowing the Commission to act promptly to protect against current cyber threats as well as future cyber or other national security threats. Full Testimony