**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.

**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**

**"Protecting the Electric Grid from Cyber Security Threats"**

**September 11, 2008**

## Introduction and Summary

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to speak here today about cyber and other national security threats to our Nation's electrical grid, and the need for legislation allowing the Federal Energy Regulatory Commission (FERC or the Commission) to address those threats quickly and effectively. I appreciate the Subcommittee's attention to this critically important issue.

The Energy Policy Act of 2005 (EPAct 2005) gave the Commission certain responsibilities for overseeing the reliability of the bulk power system. The bulk power system is defined to include facilities and control systems necessary for operating an interconnected transmission network (or any portion thereof), and electric energy from generation facilities needed to maintain transmission system reliability. EPAct 2005 authorized the Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the bulk power system. Under this framework, reliability standards are developed and proposed to the Commission by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC) through 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. The Commission is well underway in implementing the new law, including now having in place an initial set of cyber security standards with varying implementation dates. Much progress has been made in the past three years. However, more work needs to be done, both with respect to improving those cyber security standards and possibly adding new ones.

In my view, FERC does not have sufficient authority to guard against national security threats to reliability of the electric system. Legislation should be enacted allowing the Commission to act quickly to protect against current cyber threats as well as future cyber or other national security threats.

**Background**

In EPAct 2005, the Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 requires the Commission to select an ERO that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission

review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter. The Commission also may initiate enforcement on its own motion.

The Commission has implemented section 215 diligently. Within 180 days of enactment, the Commission adopted rules governing the reliability program. In mid-2006, it approved NERC as the ERO. In March 2007, the Commission approved the first set of national mandatory and enforceable reliability standards. In April 2007, it approved eight regional delegation agreements to provide for development of new or modified standards and enforcement of approved standards by Regional Entities.

In exercising its new authority, the Commission has interacted extensively with NERC and the industry. The Commission also has coordinated with other federal agencies, such as the Department of Homeland Security, the Department of Energy, the Nuclear Regulatory Commission, and the Department of Defense. Also, the Commission has established regular communications with regulators from Canada and Mexico regarding reliability, since the North American bulk power system is an interconnected continental system subject to the laws of three nations.

**Cyber Security Standards Approved Under Section 215**

Section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk power system including "cybersecurity protection." Section 215 defines reliable operation to mean operating the elements of the bulk power system within certain limits so instability, uncontrolled separation, or cascading failures will not occur "as a result of a sudden disturbance, including a cybersecurity incident." Section 215 also defines a "cybersecurity incident" as a "malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

In August 2006, NERC submitted eight new cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009, and full compliance with the CIP standards would not be mandatory until 2010.

On January 18, 2008, the Commission issued a Final Rule approving the CIP Reliability Standards and concurrently directed NERC to develop modifications addressing specific concerns, such as the breadth of discretion left to utilities by the standards. For example, the standards state that utilities "should interpret and apply the

reliability standard[s] using reasonable business judgment." Similarly, the standards at times require certain steps "where technically feasible," but this is defined as not requiring the utility "to replace any equipment in order to achieve compliance." Also, the standards would allow a utility at times not to take certain action if the utility documents its "acceptance of risk." To address this, the Final Rule directed NERC, among other things: (1) to develop modifications to remove the "reasonable business judgment" language and the "acceptance of risk" exceptions; and, (2) to develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception. A further example of this discretion involved the utility's ability to determine which of its facilities would be subject to the cyber security standards. For these requirements, the Commission addressed its concerns by requiring independent oversight of a utility's decisions by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the Commission. However, until such time as the standards are modified by the ERO through its stakeholder process, approved by the Commission, and implemented by industry, the discretion remains.

**Current Process to Address Cyber or Other National Security Threats to the Bulk Power System**

As an initial matter, it is important to recognize how mandatory reliability standards are established under section 215. Under section 215, reliability standards are developed by the ERO through an open, inclusive, and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability matter, including cyber security threats. However, the NERC process typically takes years to

develop standards for the Commission's review. In fact, the cyber security standards approved by FERC took the industry approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for industry comment, are open, and are generally based on the procedures of the American National Standards Institute (ANSI). The NERC process is intended to develop consensus on both the need for the standard and on the substance of the proposed standard. Although inclusive, the process is relatively slow and cumbersome.

Key steps in the NERC process include: nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with approval requiring a quorum of votes by 75 percent of the ballot pool and affirmative votes by two-thirds of the weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; voting by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. NERC-approved standards are then submitted to the Commission for its review.

Generally, the procedures used by NERC are appropriate for developing and approving reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process is a strength of the process as it relates to most reliability standards. However, it can be

an impediment when measures or actions need to be taken on a timely basis to effectively address threats to national security.

The procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action. If a significant vulnerability in the bulk power system is identified, procedures used so far for adoption of reliability standards take too long to implement effective corrective steps.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address a reliability vulnerability within 60 days. Also, NERC's rules of procedure include a provision for approval of urgent action standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice.

Even a reliability standard developed under the urgent action provisions would likely be too slow in certain circumstances. Faced with a cyber security or other national security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months or years. That would not be feasible under the urgent action process. In the meantime, the bulk power system would be left vulnerable to a known national

security threat. Moreover, existing procedures, including the urgent action procedure, would widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, the proposed standard submitted to the Commission may not be sufficient to address the vulnerability. As noted above, when a proposed reliability standard is submitted to FERC for its review, whether submitted under the urgent action provisions or the usual process, the agency cannot modify such standard and must either approve or remand it. Since the Commission may not modify a proposed reliability standard under section 215, we would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

**NERC's "Aurora" Advisory and Subsequent Actions**

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take voluntary action to guard against cyber or other vulnerabilities. That approach provides for quicker action, but any such advisory is not mandatory, and should be expected to produce inconsistent and potentially ineffective responses. That was our experience with the response to an advisory issued last year by NERC regarding an identified cyber security threat referred to as the "Aurora" threat. Reliance on voluntary measures to assure national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards cannot assure reliability of the bulk power system.

In response to the Aurora threat, NERC issued an advisory to certain generator owners, generator operators, transmission owners, and transmission operators. According to NERC, this advisory identified a number of short-term measures, mid-term measures and long-term measures designed to mitigate the cyber vulnerability. NERC asked the recipients to voluntarily implement the measures within specific time periods. NERC also sent a data request to industry members to determine compliance with the advisory. That data request was limited in scope, however, asking only that industry members indicate if their mitigation plans are "complete," "in progress," or "not performing."

The Commission determined that the information sought by NERC in the above data request was not sufficient for the Commission to discharge its duties under section 215 because it did not provide sufficient details about individual mitigation efforts for the Commission to be certain that the threat had been addressed. For example, it did not provide information such as what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken – and, if certain actions were not being taken, why not.

In October 2007, the Commission sought emergency processing by the Office of Management and Budget (OMB) of a proposed directive to require utilities to provide information immediately on their mitigation efforts. OMB posted the proposal for public comment in December 2007, and received several comments raising issues about the Commission's ability to protect sensitive information from public disclosure. The Commission ultimately asked OMB to hold the proposal in abeyance while Commission

staff asked a sampling of generation and transmission entities to voluntarily discuss with staff their compliance with the Aurora advisory. In February, Commission staff began interviewing them. Commission staff has conducted 30 detailed interviews with a variety of electric utilities geographically dispersed across the contiguous 48 states, to assess the state of the industry's protection against remote access cyber vulnerabilities, including the Aurora vulnerability. Each interview typically lasted six to eight hours and utilities voluntarily participated. The utilities were well prepared with documents to explain their actions, and were very cooperative in responding to staff questions. Staff found a wide range of equipment, configurations and security features implemented by the utilities. Several observations can be made based on the interviews.

All of the companies selected by the Commission fully cooperated in the interviews. We learned that there was a broad range of compliance based on individual interpretations of the threat that affected the application of the recommended mitigation measures. In fact, all of the utilities interviewed by the Commission requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, FERC staff has determined that although progress has been made by almost every entity it interviewed, much work remains to be done and, in large part, the Aurora threat remains.

While NERC can issue an alert, as it did in response to the Aurora vulnerability, compliance with these alerts is voluntary and subject to the interpretation of the individual utilities. Because an alert is voluntary, it may tend to be general in nature, and

lack specificity. Further, as Commission staff has found with the Aurora alert, such alerts can cause uncertainty about the specific strategies needed to mitigate the identified vulnerabilities and the assets to which they apply.

Damage from cyber attacks could be enormous. All of the electric system is potentially subject to cyber attack, including power plants, substations, transmission lines, and local distribution lines. 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. The harm could extend not only to the economy and the health and welfare of our citizens, but even to the ability of our military forces to defend us, since many military installations rely on the bulk power system for their electricity. The cost of protecting against cyber attacks is difficult to estimate but, undoubtedly, is much less than the damages and disruptions that could be incurred if we do not protect against them.

The need for vigilance may increase as new technologies are added to the bulk power system. For example, “smart grid” technology may provide significant benefits in the use of electricity. These include the ability to manage not only energy sources, but also energy consumption, in the reliable operation of the Nation’s electric grid. However, smart grid technology will also introduce many potential access points to the computer systems used by the electric industry to operate the electric grid. Security features must be an integral consideration. To some degree, this is similar to the banking industry allowing its customers to bank on line, but only with appropriate security protections in

place. As the "smart grid" effort moves forward, steps will need to be taken to ensure that cyber security protections are in place prior to its implementation. The challenge will be to focus not only on general approaches but, importantly, on the details of specific technologies and the risks they may present.

**Key Elements of Needed Legislation**

In my view, 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. Though the nature of the threat is different, the consequences are identical. Widespread disruption of electric service can quickly undermine the U.S. government and economy and endanger the health and safety of millions of citizens. Given the national security dimension to this threat, 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 certain information from public disclosure. Our 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.

I ask Congress to enact legislation, outside of section 215, containing the following major elements. The bill should direct the Commission to establish, after notice and opportunity for comment, interim reliability measures to protect against the threats identified in NERC's "Aurora" advisory and related remote access issues. These interim measures could later be replaced by reliability standards developed, approved and implemented under the section 215 process. The bill also should allow the Commission, upon directive by the President (directly or through the Secretary of Energy), to issue emergency orders directing actions necessary to protect the reliability of the bulk power system against an imminent cyber security or other national security threat. Significantly, FERC could only act upon such a directive. This reflects the reality that the President and national security and intelligence agencies such as DOE are in a better position than the Commission to determine the nature of a national security threat, while the Commission has the expertise to develop appropriate interim reliability measures.

I emphasize that the latter authority should apply not only to cyber security threats but also to other national security threats. Intentional physical malicious acts (targeting, for example, critical substations and generating stations) can cause equal or greater destruction than cyber attacks and the Commission should have no less ability to address them when an emergency arises. This additional authority would not displace other means of protecting the grid, such as action by federal, state and local law enforcement and the National Guard, but the Commission has unique expertise regarding the reliability of the grid, the consequences of threats to it and the measures necessary to safeguard it. If particular circumstances cause both FERC and other governmental

authorities to require action by utilities, FERC will coordinate with other authorities as appropriate.

The bill should allow measures or actions that might be imposed under this new authority to be replaced by standards developed under section 215 where applicable. For example, there may be circumstances in which use of the section 215 process would not be applicable, such as when targeted and/or temporary measures are necessary based on specific threat information. Also, the Commission should be allowed to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of this authority.

The bill also should address the following details. First, the bill should allow the Commission to take emergency action before a cyber or other national security incident has occurred, if there is a likelihood of a malicious act or a substantial possibility of disruption due to such an act. In order to protect the grid, it is vital that the Commission be authorized to act before a cyber attack. It is equally necessary that the threshold for a threat determination not be so high as to be insurmountable. Second, with respect to the Aurora and related cyber threats of which we are aware today, the Commission should be permitted and directed, after notice and comment, to require owners, users and operators of the bulk power system to take adequate measures to address those threats, and those measures should remain in effect until the measures are no longer necessary, for example, if replacement standards are approved and implemented under section 215. Third, with respect to other actions or measures the Commission might order to address future imminent threats to reliability, any time-triggered sunset provision applicable to

emergency actions ordered by the Commission should allow an exception if the President (directly or through the Secretary of Energy) reaffirms the continuing nature of the threat. In the event that the action is determined to be no longer necessary or if the measures or actions ordered by the Commission are replaced by standards approved and implemented under section 215, the Commission should issue a "discontinuance" order.

Finally, Congress should be aware of the fact that if additional reliability authority is limited to the "bulk power system," as defined in the FPA, it would exclude protection against reliability threats and emergency actions involving Alaska and Hawaii and possibly the territories, including any federal installations located therein. The current interpretation of "bulk power system" also would exclude some transmission and all local distribution facilities, including virtually all of the grid facilities in large cities such as New York and Washington, D.C., thus precluding possible Commission action to mitigate imminent cyber or other national security threats to reliability that involve such facilities and major population areas.

**Conclusion**

The Commission's authority is not adequate to address urgent cyber or other national security threats. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Congress should address this risk now.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.