

**Testimony of The Honorable Joseph T. Kelliher
Chairman
Federal Energy Regulatory Commission**

**Before the
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology
Committee on Homeland Security
United States House of Representatives**

**Implications of Cyber Vulnerabilities on the
Resiliency and Security of the Electric Grid**

May 21, 2008

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to speak with you today about the cyber vulnerabilities of the Nation's bulk power system. I appreciate the Subcommittee's attention to this critically important issue.

The Energy Policy Act of 2005 (EPAAct 2005) made the Federal Energy Regulatory Commission (FERC or Commission) responsible for overseeing the reliability of the bulk power system. EPAAct 2005 authorized the Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the Nation's bulk power system. Under the new statutory framework, reliability standards are proposed by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC) to the Commission for its review. The Commission must either approve the proposed standards or remand them to NERC. The Commission and NERC are well underway in implementing the new law, including now having in place an initial set of mandatory cyber security standards with varying effective 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 addition, the Commission has made substantial progress in examining whether industry has in place adequate mitigation to address the cyber security vulnerability, known as Aurora, which was raised at the Subcommittee's last hearing on cyber security threats to the transmission grid.

Protecting the interstate bulk power system against cyber security threats is critical to the welfare of our Nation's citizens. It is therefore appropriate to examine whether sufficient Federal authority exists to take timely and effective action to protect against such threats, particularly in emergency circumstances. In my view, FERC currently does not have sufficient authority to adequately guard against cyber security threats to reliability of the bulk power system.

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. In anticipation of reliability legislation being passed, it established a reliability group at the agency even before the passage of EPAct 2005. Within 180 days of enactment, the Commission adopted rules governing the reliability program. In the summer of 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. The Commission has since approved eight additional reliability standards.

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

Testimony, J. Kelliher

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. NERC proposed an implementation plan under which certain requirements would be “auditably compliant” beginning by mid-2009 and the others would be so by the end of 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.

The eight CIP standards contain over 160 requirements and sub-requirements. Generally, the CIP standards will require the following actions when fully implemented at the end of 2010:

Critical Cyber Asset Identification: requires the identification of an entity’s critical assets and critical cyber assets using a risk-based assessment methodology.

Security Management Controls: requires an entity to develop and implement security management controls to protect critical cyber assets.

Personnel and training: requires personnel with access to critical cyber assets to go through identity verification, criminal background checks and employee training.

Electronic Security Perimeters: requires the identification and protection of electronic security perimeters and access points. The security perimeters are to encompass the critical cyber assets.

Physical Security of Critical Cyber Assets: requires the creation and maintenance of a physical security plan that ensures all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

Systems Security Management: requires an entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within the perimeter.

Incident Reporting and Response Planning: requires the identification, classification and reporting of cyber security incidents related to critical cyber assets.

Recovery Plans for Critical Cyber Assets: requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

In the Final Rule, the Commission stated its concern with 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 to, among other things:

Develop modifications to the CIP reliability standards to remove the “reasonable business judgment” language.

Develop modifications to remove “acceptance of risk” exceptions from the CIP reliability standards.

Develop specific conditions that a responsible entity must satisfy to invoke the “technical feasibility” exception. This allows flexibility and customization of implementation of the CIP reliability standards in a controlled manner that includes external oversight and audit.

Provide additional guidance regarding the development of a risk-based assessment methodology for the identification of critical assets.

For certain other requirements in the CIP standards, the Commission addressed its concern about discretion by requiring external oversight of utility decisions, such as critical assets lists. This oversight could be provided by industry entities with a “wide-area view,” such as reliability coordinators or the Regional Entities, subject to the review of the Commission.

Current Process to Protect Cyber Security of Bulk Power System

In my view, section 215 is an adequate statutory foundation to protect the bulk power system against most reliability threats. However, the cyber security threat is different. It is a national security threat that may be posed by foreign nations, or others intent on undermining 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. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, 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.

Section 215 Process

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 and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability vulnerability, including cyber security threats. However, the NERC process can take years to develop standards for the Commission's review. In fact, the cyber security standards approved by the agency last January took the industry approximately 3 years to develop.

Section 215 relies on the ERO to develop and submit proposed reliability standards. NERC's procedures for doing so 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 not nimble.

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 based on 75 percent of total votes and two-thirds of 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.

For the first set of reliability standards proposed by NERC and for the CIP standards, the Commission began its process by issuing a staff assessment of the proposed standards and allowing public comment on the assessment. Based on its consideration of those comments, the Commission then issued a Notice of Proposed Rulemaking identifying the Commission's proposed actions and allowing additional opportunities for public comment. After considering these additional comments, the Commission issued a Final Rule approving the proposed standards and requiring NERC to prospectively modify them using its standards development process, thereby engaging industry.

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 a weakness in the development of cyber security standards, given the nature of the threat.

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 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 an identified reliability vulnerability within 60 days. 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, 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, FERC may need to act decisively in hours or days, rather than 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 cyber security threat. Moreover, existing procedures, including the urgent action procedure, would widely publicize the vulnerability and the possible 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 could remain vulnerable for a prolonged period.

NERC Advisories

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take action to guard against cyber vulnerabilities. That approach provides for quicker action, but any such advisory is voluntary, and should be expected to produce inconsistent responses. That was our experience with the response to an advisory issued last year by NERC regarding an identified cyber security threat. Since the grid is interconnected, those inconsistencies can retard cyber security measures. Reliance on voluntary measures to assure cyber security is fundamentally inconsistent with the conclusion Congress reached during enactment of the Energy Policy Act, namely that voluntary standards cannot assure reliability of the bulk power system.

In response to the risk of cyber attack identified last year as Aurora, this Subcommittee convened a hearing on October 17, 2007. Mr. Joseph H. McClelland, the Director of the

Commission's Office of Electric Reliability, testified at that hearing. NERC reported that it issued an advisory to 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. 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. Therefore, on October 23, 2007, the Commission provided notice to the Office of Management and Budget (OMB) that it intended to immediately issue a directive requiring all generator owners, generator operators, transmission owners, and transmission operators that are registered by NERC and located in the United States to provide to NERC certain information related to actions they have taken or intend to take to protect against the cyber vulnerability; this would allow the Commission to review the mitigation plans at a central location to be certain that the vulnerability had been addressed. The Commission requested emergency processing of this proposed information collection. After receiving clearance from OMB, the Commission issued a Notice of Proposed Information Collection and Request for Comments (Notice). Comments were due on January 14, 2008.

The Commission received seven sets of comments in response to the Notice, including joint comments filed by four industry trade associations: American Public Power Association, Edison Electric Institute, National Rural Electric Cooperative Association, and the Electric Power Supply Association. These trade associations represented the majority of entities that would be required to respond to the proposed information collection. A common concern among the commenters was the need to ensure the confidentiality of sensitive information that would be provided in response to the proposed information collection. Commenters urged that the Commission implement additional security measures to safeguard the collected information. Commission staff met with trade association representatives to discuss these concerns and how they might be addressed. Rather than experience further delays by answering these objections to the proposed mandatory information collection, it was determined that staff would first work with industry groups to develop a plan to informally gather information, on a voluntary basis, regarding the status of compliance with NERC's Aurora advisory. In February, Commission staff began performing interviews with a stratified sampling of electric utilities concerning their compliance with the Aurora advisory. These interviews are continuing as of this date.

Commission staff has conducted over 20 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. The utilities were selected to encompass both large and small companies, and a mixture of generating companies, transmission companies, and mixed-asset companies. The sample of companies included both investor-owned utilities and cooperative organizations. Interviews with publicly-owned utilities and municipal organizations are planned in the near future. 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.

Topics discussed included the use of passwords and other forms of access controls, means of authenticating users, physical security of cyber assets, means of communicating, vendor access, access revocation, the use of firewalls and intrusion detection/prevention devices, vulnerability assessments, the ways in which communications devices are utilized, as well as the prevalence and functionality of digital control devices. Staff found a wide range of equipment, configurations and security features implemented by the utilities interviewed. While staff intends to perform more interviews, there are several observations that can be made based on the interviews to date.

All of the companies selected by the Commission fully cooperated in the interviews. We learned that no company we interviewed ignored the Aurora advisory, although we did find there was a broad range of compliance based on individual interpretations of the threat and 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 every entity it interviewed, much work remains to be done.

While NERC can issue an alert, as it did in response to the Aurora vulnerability, compliance with these alerts is voluntary. 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.

Conclusion

The Congress made FERC responsible for overseeing the reliability of the bulk power system, but it provided specific restrictions on the procedures to be used to develop and put into effect mandatory reliability standards. Section 215 is an adequate basis to protect the bulk power system against most reliability threats, and for that reason I do not believe there is a need to amend section 215. However, I believe a different statutory mechanism is needed to protect the grid against cyber security threats, given the nature of

these threats. One approach would allow the Commission to directly establish interim reliability standards that are mandatory and enforceable upon a finding by a national security or intelligence agency that there is a national security threat to the bulk power system. This narrowly tailored approach would ensure that reliability of the bulk power system can be protected until the ERO reliability standards development process can create a permanent reliability standard. It also would provide that the authority be used rarely, in instances when other appropriate agencies determine that a threat is real and the Commission determines existing standards to be inadequate. It also may be necessary to authorize the Commission to protect certain information from disclosure, if its release could have significant adverse effect on the health and safety of the public or the common defense or national security.

The full range of cyber security risks to the bulk power system are not known, and new risks will continue to arise. I believe we should not allow the Nation's bulk power system to be vulnerable to a known national security threat while waiting months or years for a reliability standard to be developed and submitted to the Commission for review. At the same time, reliance on a voluntary alert issued by NERC similarly does not provide adequate assurance that steps will be taken in sufficient time to address a known vulnerability. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, 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.

The Commission has taken, and will continue to take, action to protect the bulk power system from cyber vulnerabilities. We continue to work with national security agencies to understand the nature of the threats facing the bulk power grid. We have established mandatory cyber security standards under the section 215 process and have directed improvements in approved standards over time. We also continue to review the industry response to the NERC advisory on the Aurora threat, and may review the response to any future such advisories. But I do not want to leave you under the impression that these steps adequately protect the bulk power system against cyber attacks.

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