Testimony of

Joseph McClelland

Director, Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426
(202) 502-8600

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

The Cyber Threat to Control Systems: Stronger Regulations Are Necessary to Secure the Electric Grid.

October 17, 2007

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to appear before you to discuss the cyber threat to the electric grid's control systems. My name is Joseph McClelland. I am the Director of the new Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (Commission). The OER's mission is to help protect and improve the reliability and security of the Nation's bulk-power system through effective regulatory oversight as established in the Energy Policy Act of 2005 (EPAct 2005). I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

My testimony summarizes the Commission's recent efforts to improve the security of the Nation's electric power system. Congress's recent legislation has greatly expanded the Commission's ability to anticipate and respond to cybersecurity threats to a critical component of the Nation's infrastructure, the interstate bulk-power system. The Commission has met its statutory deadlines and provided a solid foundation for ongoing regulatory efforts. Ongoing efforts focus on the approval of Reliability Standards governing the planning and operation of the interstate bulk-power system as mandatory rules with appropriate penalties, subject to the Commission's oversight and approval.

The Commission continues to work with the North American Electric Reliability Corporation (NERC) to protect the bulk-power system from cybersecurity threats. NERC has proposed cybersecurity standards for the industry and the Commission has issued a notice of proposed rulemaking addressing these standards. The Commission is reviewing comments on these standards and is committed to ensuring that the resulting standards are consistent with and effectively implement recommendations proposed in response to the 2003 blackout affecting the Northeast United States and Canada.

The Commission is assessing its options for immediately and effectively addressing urgent cybersecurity risks to the electric system. The Reliability Standards process, which focuses on consensus from industry representatives, typically takes considerable time to implement. If the Commission determines that its authority to promptly address cybersecurity risks is inadequate, it will seek additional legislation.

As the Commission meets its responsibilities under EPAct 2005 to protect the Nation's bulk-power system, it is encountering new staffing and program needs. In particular, the Commission needs to hire more engineers to review and enforce Reliability Standards affecting the hundreds of entities that use the bulk-power system. Therefore, the Commission has requested additional budget

authority for 2008, the costs of which would be recovered through the Commission's existing self-funding process.

Background

In August 2005, Congress enacted EPAct 2005 entrusting the Commission with a major new responsibility to oversee mandatory, enforceable Reliability Standards for the electric grid. This authority is in section 215 of the Federal Power Act (FPA). Section 215 requires the Commission to select an Electric Reliability Organization (ERO). The ERO 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. 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. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed Reliability Standards or modifications 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, FPA 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 but, for most violations, will only review the enforcement actions of the ERO.

The Commission is qualified to perform all of these tasks and, in anticipation of reliability legislation being passed, it established a reliability group at the agency even before the passage of EPAct 2005. Commission staff played a key role in the U.S.-Canada Power System Outage Task Force formed to investigate the August 2003 blackout that affected eight states, one province and an estimated 50 million people in the U.S. and Canada. When the Task Force issued its report in April 2004 (Blackout Report), the Commission acted quickly to implement the report's recommendations addressed to the Commission. For example, the Commission announced that no new independent system operator or regional transmission organization would be approved until its reliability capabilities were functional. The Commission also adopted a policy statement on several other issues, such as recovery of prudent reliability costs, cooperation with the States, and the interpretation of reliability-related provisions in transmission tariffs. On this last point, the Commission stated that tariff requirements to follow "good utility practice" would include compliance with the then-voluntary

standards developed by NERC's predecessor, the North American Electric Reliability Council.

With this experience, the Commission has been able to implement FPA section 215 diligently. 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. And, just last month, the Commission's Division of Reliability in the Office of Energy Markets and Reliability was established as its own program office, the OER, to reflect the growing importance of the Commission's reliability responsibilities.

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 and the Nuclear Regulatory Commission. And, 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.

The Commission's Proposed Cybersecurity Regulations

FPA section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk-power system and for "cybersecurity protection." Section 215 defines reliable operation to mean operating the elements of the BPS within certain limits so instability, or 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 2003, before the passage of EPAct 2005, NERC approved the "Urgent Action 1200" standard (UA 1200), the first comprehensive, although temporary, cybersecurity standard for the electric industry. This voluntary standard applied to control areas (i.e., balancing authorities responsible for ensuring that a specific area's supply matches demand at any moment in time), transmission owners and operators, and generation owners and operators that perform certain functions.

Specifically, UA 1200 established a self-certification process relating to the security of system control centers.

In May 2006, NERC approved eight new cybersecurity standards to supersede UA 1200. These new standards, known as the Critical Infrastructure Protection (CIP) standards and discussed below, are broader in scope and applicability than UA 1200 and, if approved by the Commission, would be mandatory. In August 2006, NERC submitted the new standards to the Commission for approval under FPA section 215. Citing the expanded scope of facilities and entities covered by the CIP standards, and the investment in security upgrades required in many cases, NERC proposed an implementation plan under which certain requirements would be "auditably compliant" by 2009 and the others would be so by 2010.

In December 2006, the Commission issued an assessment by its staff of NERC's proposed CIP standards, and allowed 60 days for public comments. The staff's assessment was limited to a technical review, and made no final determinations on compliance with FPA section 215's legal requirements.

After receiving and analyzing the nearly 500 pages of comments from 38 entities, the Commission issued a Notice of Proposed Rulemaking in July 2007 proposing to adopt the CIP standards subject to further comment from the public. The Commission also proposed to concurrently direct NERC to develop modifications addressing specific concerns identified by the Commission.

The eight CIP standards contain over 160 requirements. Generally, the CIP standards would require the following actions:

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.

Public comments comprising more than 800 pages from 69 entities on the Commission's proposed actions were filed as of October 5. The Commission's staff has begun reviewing these comments, and the Commission intends to take final action expeditiously.

One of the Commission's goals is to ensure that the cybersecurity standards are consistent with the lessons learned from the August 2003 blackout. Thirteen of the 46 Blackout Report recommendations relate to cybersecurity. See the Blackout Report at pp. 163-69. They address topics such as strict control of physical and electronic access to operationally sensitive equipment; capability to detect wireless and remote wireline intrusion and surveillance; and improvement and maintenance of cyber forensic and diagnostic capabilities. The Blackout Report recommendations are a sound basis for action.

The Commission recognizes that the CIP standards must strike a reasonable balance. Overly prescriptive standards may become a "one size fits all" solution despite the significant differences in system architecture, technology and risk profile. However, CIP standards lacking sufficient detail will provide little useful direction, make compliance and enforcement difficult, allow flawed implementation and result in inadequate protection.

A major concern with cybersecurity is the prevalence in the industry of "legacy equipment" which may not be readily adaptable for purposes of cybersecurity protection. If this equipment is left vulnerable, it could be the focal point of efforts to disrupt the grid. Replacing this equipment or retrofitting it to incorporate cybersecurity protection could be costly. But a successful cyber attack could damage our bulk-power system and economy in ways that cost far more.

This risk often may justify retrofitting the legacy equipment, adding a perimeter of defensive security measures or replacing the equipment before its useful life ends.

In its July 2007 Notice of Proposed Rulemaking, the Commission stated its concern with the breadth of discretion left to utilities by NERC's proposed CIP standards. For example, NERC's 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, NERC's proposal would allow a utility at times not to take certain action if the utility documents its "acceptance of risk." The Commission proposed to direct NERC to modify the standards to remove the terms "reasonable business judgment" and "acceptance of risk" while narrowing "technically feasible."

For certain other requirements in the CIP standards, the Commission proposed to address this concern about discretion by requiring external oversight of utility decisions. 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.

The National Institute of Standards and Technology (NIST) has commented that its cybersecurity standards are more advanced and could provide a model for improvements to the CIP standards. NIST has recommended that the Commission consider a transition to standards identical to, consistent with, or based on NIST standards and guidelines. The Commission's proposal so far is to not require incorporation of the NIST standards and guidelines. However, the Commission has said it would expect NERC to monitor the development and implementation of the NIST standards to determine if they would provide better protection. Certain federal entities, such as the Tennessee Valley Authority and Western Area Power Administration, are required to comply with both the NIST standards and the CIP standards, and thus may be able to provide unique insights on this issue. The Commission expressed its expectation that NERC will seek and consider comments from these federal entities on the effectiveness of the NIST standards versus the CIP standards. Any provisions in the NIST standards that will better protect the bulk-power system should subsequently be addressed in the standards development process as improvements to the CIP standards. In addition to this consideration, the Commission proposes to revisit this issue in future proceedings as part of a continuing evaluation of existing standards, the need for new standards, or as part of assessing NERC's performance as the ERO.

Confronting Urgent Risks

The procedures used so far for adoption of Reliability Standards have allowed multiple opportunities for industry and public input and taken significant time, as explained below. However, urgent risks may at times require immediate action, and the Commission currently is exploring the scope of its authority under existing law to take swift and effective action to prevent opportunities for cyber attacks or address other critical matters.

FPA 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, 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 and can take years to develop standards for the Commission's review.

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 NERC staff; drafting or redrafting of the standard by an assigned team; 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 currently under consideration, 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 will issue a "Final Rule," adopting or modifying its proposed actions.

Generally, the procedures used by NERC and the Commission are appropriate in allowing extensive opportunities for industry and public comment. The public and our economy depend critically on having a reliable supply of electricity, and Reliability Standards usually should be adopted only after thorough and open vetting of all relevant considerations.

Certain circumstances, however, may require immediate action. If a significant vulnerability in the bulk-power system is identified, procedures used so far for adoption of Reliability Standards may take too long to implement corrective steps. Also, those procedures would widely publicize the vulnerability and the possible solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

Recently, CNN broadcast a story alleging the existence of a cybervulnerability on the electric grid. The story included video of a small generating unit allegedly being damaged by a cyber attack, and also showed an economist stating that there could be a $700 billion dollar impact to our economy if generating facilities serving one-third of our Nation's electric load were disabled for three months through such attacks.

This story has prompted the Commission to reexamine its authority to quickly mitigate verified cybervulnerability risks and to protect security-sensitive information from inappropriate disclosure. If the Commission determines that it does not have adequate authority to promptly address cybersecurity risks and adequately protect security-sensitive information, or that its authority needs to be clarified, it will seek additional legislation.

The Commission Needs More Funding for Reliability

As noted above, the Commission has certified NERC as the ERO; approved the first set of mandatory and enforceable Reliability Standards (83 of NERC's initial 107 while calling for significant modifications to 56 of the 83); and approved delegation agreements between NERC and eight Regional Entities. With these steps, the Commission is well positioned to implement FPA section 215. However, more resources are needed by the Commission in all areas of reliability, including physical and cyber standards development, compliance and enforcement, investigation and analysis, and reports and assessments. In addition, the new Reliability Standards, including cybersecurity standards, will take significant work by the Commission, the ERO and the industry, and thus competition for experienced personnel, particularly engineers, is strong. Oversight of the reliability of the Nation's bulk-power system is one of the most important functions ever undertaken by the Commission and the Congress's budget support in providing necessary resources is critical.

The Commission will continue to work with the ERO and industry to strengthen Reliability Standards. Our staff will monitor and engage in the standards development process to provide timely feedback to stakeholders. NERC and industry stakeholders have requested the Commission's staff to be involved in the standards development process. We believe the process will work better if the

Commission's staff is involved from the beginning, to help ensure that necessary improvements to the standards are made timely and comport with Commission directives. This is important because section 215 does not give the Commission explicit authority to revise or write the standards. Instead, the Commission can only direct the ERO to submit a standard on a specific matter or remand a proposed standard to the ERO with directions for modification, and the standards development and revision process is lengthy.

In addition, Commission staff will participate with the Regional Entities in a number of regular compliance audits and in analyzing selected incidents on the bulk-power system. Staff also will analyze and/or prepare reports on various issues concerning the reliability and security of the bulk-power system.

The Commission has moved quickly to fulfill the Congressional intent of FPA section 215. However, after we completed the actions cited above, we came to understand better the resource needs for our new reliability responsibilities. For example, approximately 1500 U.S. utilities or users of the bulk-power system are now "registered" by NERC to comply with the Reliability Standards. The Commission's jurisdiction to implement and enforce FPA section 215 for such a large number of entities serving the entire United States bulk-power system is a significant responsibility and requires a significant commitment of resources.

Thus, in June of this year, the Commission's Chairman wrote to the Chairmen and Ranking Members of the House and Senate Appropriations Committees, seeking an additional $9 million for our reliability work in fiscal year 2008. This would provide for an additional 55 Full-Time Equivalents (FTEs) to support its reliability program. These FTEs would consist primarily of electrical engineers, power system experts, auditors and lawyers. The Commission's Chairman also asked for authorization to hire electrical engineers non-competitively up to the GS-15 level, and to hire six additional executive senior level (SL) staff in support of its reliability program. As you may know, the Commission is a self-supporting agency and would recover the additional appropriations through fees and annual charges, as it does all of its costs, and will operate at no net cost to the taxpayer. I encourage you to support these requests by the Commission.

Conclusion

I stress that the Commission is taking all the steps it can to protect the bulk-power system and is dedicated to fulfilling Congress's goals. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.