Testimony of Joseph McClelland
Director, Office of Electric Reliability
Federal Energy Regulatory Commission
Before the Committee on Energy and Natural Resources
United States Senate
May 7, 2009

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to appear before you to discuss the cyber security of the electric grid. My name is Joseph McClelland. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). The Commission's role with respect to reliability is to help protect and improve the reliability of the Nation's bulk-power system through effective regulatory oversight as established in the Energy Policy Act of 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 oversight of the reliability of the electric grid in the area of security, some of the Commission's actions to implement section 215 of the Federal Power Act, and some of the limitations in the Commission's authority. The Commission does not have sufficient authority to provide effective protection of the grid against cyber attacks or other security threats to reliability. As will be explained in more detail later, this is primarily due to three factors regarding the development of reliability standards under section 215; lack of timeliness, lack of ability to protect security-sensitive information,

and lack of ability to control the content of proposed cybersecurity standards. Therefore, legislation is needed and my testimony discusses the key elements that should be included in any new legislation in this area.

Background

In the Energy Policy Act of 2005 (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 Electric Reliability Organization (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." The Commission does not have authority to modify proposed standards. Rather, 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 however, does not have the authority to modify or author a standard but must depend upon the ERO to do so.

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 the North American Electric Reliability Corporation (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 and meetings with regulators from Canada and Mexico regarding reliability, since the North American bulk power system is an interconnected continental system subject to the varied regulatory regimes of three nations.

Cyber Security Standards Approved Under Section 215

An important part of the Commission's responsibility to oversee the development of reliability standards involves cyber security. 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 proposed cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Each of these standards contains layers of multiple requirements. 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, after issuing both a staff preliminary assessment and notice of proposed rulemaking, the Commission issued a Final Rule approving the CIP Reliability Standards and concurrently directed NERC to develop significant 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" that might be placed on the bulk-power system. 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. NERC and the industry are working on proposed modifications to address these two issues. 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 and critical facilities will be left unprotected.

A good example of the discretion implicit in the existing cyber security

standards involves the utility's ability to determine which of its facilities would be subject to them. In the Final Rule, 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. This revision to the standards is subject to approval by the affected stakeholders in the standards development process and therefore has not yet been presented to the Commission. NERC recently conducted a survey on this issue which seems to validate the Commission's concern and original directives by demonstrating that a significant percentage of owners and operators do not believe they own or operate critical cyber assets. For example, NERC stated that only 29% of generation owners and generation operators reported at least one critical asset, though it is unclear from NERC's data what portion of the Nation's generation capacity that 29% represents, or what portion the designated critical assets represent. Thus, it is not clear, even today, what percentage of critical assets and their associated critical cyber assets has been identified. It is clear, however, that this issue is serious and represents a significant gap in cybersecurity protection.

Current Process to Address Cyber or Other National Security Threats to Reliability

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 or vulnerabilities. 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. 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, cumbersome and unpredictable regarding its responsiveness to the Commission's directives.

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; approval 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. This standards development process requires public

disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues at-hand, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments.

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 can be 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 to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information.

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. Moreover, 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 even 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 or threat. 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, it 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.

Finally, the open and inclusive process required for standards development is not consistent with the need to contain security-sensitive information. For instance, a SAR would normally detail the need for the standard as well as the proposed mitigation to address the issue. Subsequent drafts of the standard would consider how effectively it addresses the cyber security matters and what objections or revisions are proposed by the stakeholders resulting in a final version that would be filed with the Commission for review. Potential adversaries would have the ability to monitor these developments and alter their actions as necessary to preserve an effective attack vector.

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 the Commission's experience with the response to an advisory issued in 2007 by NERC regarding an identified cyber security threat referred to as the "Aurora" threat. 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. Also, an alert can be general in nature and lack specificity. For example, 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. 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.

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. In fact, a recent Defense Science Board report concluded that "critical missions at military installations are vulnerable to loss from commercial power outage and inadequate backup power supplies."[1] The cost of protecting against cyber attacks is difficult to estimate but, undoubtedly, is

[1] Report of the Defense Science Board Task Force on DoD Energy Strategy "More Fight – Less Fuel", February 2008.

much less than the damages and disruptions that could be incurred if we do not protect against them.[2]

The need for vigilance may increase as new technologies are added to the bulk power system. For example, "smart grid" technology will provide significant benefits in the use of electricity. These include the promised ability to manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a much larger number of devices located outside of controlled utility environments, which will introduce many potential access points. 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. Security features must be an integral consideration, as the Commission stated in a recent proposed policy statement on smart grid. 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 provides an adequate statutory foundation for the ERO to develop reliability standards for the bulk power system. However, the

[2] As an example, the US Canada Joint Task Force on the August 2003 Blackout concluded that the outage that affected over 50,000,000 citizens and was estimated to cost between $4 and $10 billion dollars in the United States.

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 protective relay maintenance practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as 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. 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.

Any new legislation should address several key concerns. First, legislation should allow the Commission to take action before a cyber or other national security incident has occurred to prevent a significant risk of disruption to the grid due to such an incident. In order to protect the grid, it is vital that the Commission be authorized to act before an attack. Second, any legislation should allow the Commission to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of this authority. It

should also allow the Commission to protect such information when the Commission issues orders under any new authority. Third, it is important that Congress be aware that if additional reliability authority is limited to the "bulk power system," as defined in the FPA, it would exclude protection against attacks 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., thus precluding possible Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. Finally, legislation should address not only cyber security threats but also other national security threats to reliability.

The Joint Staff draft bill is one approach that would largely rectify the inadequacies in existing federal authority to address cyber threats to the electric grid. It gives the Commission authority to issue rules or orders that are necessary to protect critical electric infrastructure from weaknesses or flaws in the design or operation of electric devices or networks that expose critical electric infrastructure to a cyber security threat. This authority to address cyber security vulnerabilities would apply to all systems or assets, whether physical or virtual, used for the generation, transmission, and distribution of electric energy that in the determination of the Commission are so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on the

security, national economic security, or national public health or safety. Thus, it would allow the Commission to act to protect against potential damage to the grid, including the grid facilities in New York City, which I referenced earlier.

As I have noted, a key concern with respect to any cyber security legislation is that the Commission must be allowed to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of its authority. This applies to information submitted to the Commission and to orders issued by the Commission, which may contain security-sensitive information. While the draft bill addresses the protection of critical infrastructure information, it could be construed to provide protection only for information voluntarily submitted to the Commission or the Secretary. Not all information submitted to the Commission or the Secretary will be submitted voluntarily, but rather may be ordered to be submitted in an agency rule or order. Additionally, the Commission or the Secretary may need to include sensitive information in the orders they issue and this information similarly should be non-public. Therefore, I recommend that the language be amended to address these issues.

I also recommend that the Joint Staff draft be amended to address not only cyber security threats but also other national security threats to reliability. Intentional physical malicious acts (targeting, for example, critical substations and generating stations) can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such

potential damage. 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.

Finally, Congress should be aware of the fact that if additional reliability authority is limited to the areas within the Commission's jurisdiction under section 215 of the FPA, it would exclude protection against reliability threats in Alaska and Hawaii and possibly the territories, including any federal installations located therein.

Conclusion

The Commission's authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. 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.