Testimony of Joseph McClelland
Director, Office of Electric Reliability
Federal Energy Regulatory Commission
Before the Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
United States House of Representatives
July 21, 2009

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to appear before you to discuss the 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 under section 215 of the Federal Power Act, and some of the limitations in Federal authority to protect the grid against physical and cyber security threats. The Commission currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. If adequate protection is to be provided, 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), 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 Commission has certified the North American Electric Reliability Corporation (NERC) as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States 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 itself 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 but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Limitations of Section 215 And The Term "Bulk Power System"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas.

Critical Infrastructure Protection Reliability Standards

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber security. 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. 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 would be mandatory in 2010. Pursuant to NERC's implementation plan for the CIP standards, the term "auditably compliant" means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" At the end of July 2009, responsible entities will provide responses to NERC's self-certification survey. Those responses will include information on their progress towards compliance with the CIP standards.

On January 18, 2008, the Commission issued a Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The Commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each

of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the Commission into phases, based on their complexity. NERC opted to resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009 and the filing is currently under review by Commission staff. The filing includes removal from the standards of the terms "reasonable business judgment" and "acceptance of risk," which the Commission found problematic, the addition of a requirement for a "single senior manager" responsible for CIP compliance, and certain other administrative and clarifying changes. The remaining phases of the CIP reliability standard revisions to respond to the Commission's directives are still under development by NERC. Currently, there are no set time frames for the remaining phases.

Identification of Critical Assets

As currently written, the CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the protection requirements of the standards. In the Final Rule, the Commission directed NERC to revise the standards to require 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, like all revisions, is subject to approval by the affected stakeholders in the standards development process and has not yet been developed or presented to the Commission. We expect this revision to be part of the remaining phases of CIP reliability standard revisions, as discussed above.

When the Commission approved the CIP reliability standards in January 2008, it also required entities under those standards to self-certify their compliance progress every six months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP-002-1. As the Commission stated in the Final Rule, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at protecting the bulk power system. The results of NERC's self-certification request showed that 31% of responsible entities responding to the survey, and only 29% of generation owners and operators, identified at least one critical asset, while about 63% of transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009. In addition, NERC is working on a guidance document that will help industry to identify their critical assets. That document is still under development, and should be completed in approximately six months. Another self-certification by industry is due to NERC at the end of July, and includes additional questions designed to obtain a better understanding

of the results from industry's critical asset identification process. Those results will help gauge how widely the CIP reliability standards have been applied.

The results of the NERC survey demonstrate that it is not clear, even today, what percentage of critical assets and their associated critical cyber assets has been identified and therefore made subject to the protection requirements of the CIP standards. It is clear, however, that this issue is serious and represents a significant gap in cyber security protection.

The NERC Process

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be 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 requires years to develop standards for the Commission's review. In fact, the existing CIP standards took 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, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in 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. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. 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

can be a strength of the process. 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 current 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, while the reliability standard procedures take too long to implement efficient and timely 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 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, a reliability standard submitted to the Commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not modify a proposed reliability standard under section 215 and must either approve or remand it, FERC 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 protect security-sensitive information. For instance, a Standard Authorization Request would normally detail the need for the standard as well as the proposed mitigation to address the issue, and the NERC-approved version of the standard would be filed with the Commission for review. This public information could help potential adversaries in planning attacks.

NERC's "Aurora" Advisory

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 allows for quicker action, but compliance with an advisory is not mandatory, and may produce inconsistent and potentially ineffective responses. Also, an alert can be general in nature and lack specificity. For example, the issuance of an advisory in 2007 by NERC, regarding an identified cyber security vulnerability referred to as "Aurora," caused 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.

Smart Grid

The need for vigilance may increase as new technologies are added to the bulk power system. For example, smart grid technology promises significant benefits in the use of electricity. These include the ability to better manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.

Smart grid applications will automate many decisions on the supply and use of electricity to increase efficiencies and ultimately to allow cost savings. Without adequate physical and cyber protections, however, this level of automation may allow adversaries to gain unauthorized access to the rest of the company's data and control systems and cause significant harm. Security features must be an integral consideration when developing smart grid technology. 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.

Regarding data, there are multiple ways in which smart grid technologies may introduce new cyber vulnerabilities into the system. For example an attacker could gain access to a remote or intermediate smart grid device and change data values monitored or received from down-stream devices, and pass the incorrect data up-stream to cause operators or automatic programs to take incorrect actions. As was mentioned previously, the potential exists for off-grid equipment to adversely affect the bulk power system through corrupted communications.

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed generation sources to turn off

during periods when load is approaching generation capacity, causing instability and outages on the bulk power system. One of the potential capabilities of the smart grid is the ability to remotely disconnect service using advanced metering infrastructure (AMI). If insufficient security measures are implemented in a company's AMI application, an adversary may be able to access the AMI system and could conceivably disconnect every customer with an AMI device. If such an attack is widespread enough, the resultant disconnection of load on the distribution system could result in impacts to the bulk power system. If an adversary follows this disconnection event with a subsequent and targeted cyber attack against remote meters, the restoration of service could be greatly delayed.

The CIP standards will apply to some, but not all, smart grid applications. The standards require users, owners and operators of the bulk power system to protect cyber assets, including hardware, software and data, which would affect the reliability or operability of the bulk power system. These assets are identified using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a smart grid device were to control a critical part of the bulk power system, it would be considered a critical cyber asset subject to the protection requirements of the CIP standards.

Many of the smart grid applications will be deployed at the distribution and end-user level so they may incorrectly be viewed as not affecting the bulk power system. For example, some applications may be targeted at improving market efficiency in ways that may not have a reliability impact on the bulk power system, such that the protection requirements of the CIP standards, as they are currently written, may not apply. However, as discussed above, these applications either individually or in the aggregate could affect the bulk power system.

The Commission and its staff currently are coordinating with a number of governmental and private sector organizations on cyber security issues surrounding smart grid technology, including the DOE Smart Grid Task Force, the NIST Domain Expert Working Groups, the Gridwise Architecture Council, and the FERC-NARUC Smart Grid Collaborative. The Commission has issued a policy statement that would strongly encourage interoperability of smart grid technologies, recognizing that cyber security is essential to the operation of the smart grid The Policy Statement stated that the Commission will require a demonstration of sufficient cyber security protections in the proposed smart grid standards to be considered in rulemaking proceedings under the Energy Independence and Security Act of 2007 (EISA), including, where appropriate, a proposed smart grid standard applicable to local distribution-related components of smart grid. The Commission also encouraged NERC to work with NIST in the development of the standards.

While the Commission is doing what it can under its jurisdiction, EISA does not make any standards mandatory and does not give the Commission authority to make or

enforce any such standards. Under current law, the Commission's authority, if any, to make smart grid standards mandatory must derive from the FPA.

Physical Security And Other Threats To Reliability

The Commission's current reliability authority does not extend to physical threats to the grid, but physical threats 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. One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because very little electronic technology existed at the time. Were the storm to happen today, according to an article in *Scientific American*, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[2] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the *Scientific American* article, and the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages.

Further, the power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced power spikes. The collapse of numerous transformers across the country could result in reduced grid functionality or even prolonged power outages.

---

[1] Graham, Dr. William R. et al, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2004).

[2] Odenwald, Sten F. and Green, James L., *Bracing the Satellite Infrastructure for a Solar Superstorm*, Scientific American Magazine (Jul. 28, 2008).

FERC staff has no data on how well the bulk power system is protected against an EMP event, and the existing reliability standards do not address EMP vulnerabilities. Further, the Commission currently does not have any specific authority to order owners and operators of the transmission grid, generation facilities and other electric facilities to protect their facilities from EMP-related events, other than the general authority to order NERC to develop a reliability standard addressing EMP. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP would involve vulnerability assessments at every level of electric infrastructure. In addition, as the reports point out, the reliable operation of the electric grid requires other infrastructure systems, such as communications, natural gas pipelines and transportation, which would also be affected by such an attack or event.

The Need for Legislation

In my view, section 215 of the Federal Power Act provides an adequate statutory foundation for the ERO to develop most reliability standards for the bulk power system. However, the nature of a national security threat by entities intent on attacking the U.S. through vulnerabilities in its electric grid 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 current legal authority is inadequate for such action. This is true of both cyber and non-cyber physical threats to the bulk power system that pose national security concerns. This lack of authority results in the electric grid being vulnerable to attacks, both physical and cyber.

Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the Commission to take action before a cyber or physical national security incident has occurred. In order to protect the grid, it is vital that the Commission be authorized to act before an attack to address vulnerabilities and threats. Second, any legislation should allow the Commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Third, it is important that Congress be aware that if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would exclude protection against attacks involving Alaska and Hawaii, including any federal installations located therein. The current interpretation of the term bulk power system also excludes some transmission and all local distribution facilities, including virtually all of the facilities in certain 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, it is important that entities be permitted to recover costs they incur to mitigate vulnerabilities and threats. The Commission currently has authority to allow recovery by entities that meet the FPA definition of "public utility." If Congress believes it appropriate, it could include in legislation a directive that the Commission establish a cost recovery mechanism for the costs associated with compliance with any FERC order issued pursuant to the emergency authority.

Finally, any legislation on national security threats to reliability should address not only cyber security threats but also intentional physical malicious acts (targeting, for example, critical substations and generating stations) and threats from an electromagnetic pulse. FERC should be granted authority to address both cyber and physical threats and vulnerabilities, primarily because FERC is the one Federal agency with any statutory responsibility to oversee reliability of the grid. 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. If particular circumstances cause both FERC and other governmental authorities to require action by utilities, FERC would coordinate with other authorities as appropriate. Additionally, any FERC authority to address threats to the grid would be based on a determination by the President or a national security agency that national security is endangered.

Conclusion

The Commission's current 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.