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 5, 2011

Mr. Chairman and Members of the Committee:

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 (FPA) and the Commission's implementation of that authority with respect to cyber security primarily through Order No. 706. I also will describe some of the current limitations in Federal authority to protect the grid against physical and cyber security threats, and also comment on the cyber security discussion draft. 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 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. The Commission recently issued Order No. 743, which directs NERC to revise its interpretation of the bulk power system to eliminate inconsistencies across regions, eliminate the ambiguity created by the current discretion in NERC's definition of bulk electric system, provide a backstop review to ensure that any variations do not compromise reliability, and ensure that facilities that could significantly affect reliability are subject to mandatory rules. NERC is currently developing its response to that order. However, it is important to note that section 215 of the FPA excludes local distribution facilities from the Commission's reliability jurisdiction, so any revised bulk electric system definition developed by NERC will still not apply to local distribution facilities.

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." Under NERC's implementation plan for the CIP standards, full compliance became mandatory on July 1, 2010.

On January 18, 2008, the Commission issued Order No. 706, the 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. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 CIP standards and directed NERC to develop additional modifications to certain of them. Pursuant to the Commission's September 30, 2009 order, NERC submitted Version 3 of the CIP standards which revised Version 2 as directed. The Version 3 CIP standards became effective on October 1, 2010. This first phase of the modifications directed by the Commission in Order No. 706, which encompassed both Version 2 and Version 3, did not modify the critical asset identification process, a central concern in Order No. 706.

On February 10, 2011, NERC initiated the second phase of the Order No. 706 directed modification, filing a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. This filing is currently under review by the Commission. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which reflects an extension of time requested by NERC.

The remaining CIP standards revisions to respond to the Commission's directives issued in Order No. 706 are still under development by NERC. It is important to note that the majority of the Order No. 706 directed modifications to the CIP standards have yet to be addressed by NERC. Until they are addressed, there are significant gaps in protection such as a needed requirement for a defense in depth posture. NERC's standards development plan filed with the Commission in April 2011 classifies these outstanding revisions to the CIP standards as "High Priority" with a targeted completion in the second quarter of 2012.

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 requirements of the standards. In Order No. 706, 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. NERC has attempted to address this directive in Version 4 of the CIP standards, which is now under review

by the Commission.

When, in Order No. 706, the Commission approved Version 1 of the CIP reliability standards, 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 Order No. 706, 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 only 29% of responding generation owners and operators identified at least one critical asset, while about 63% of the responding 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.

NERC conducted another self-certification survey of responsible entities to determine progress towards identification of critical cyber assets. It gathered information about critical assets and critical cyber assets as of December 31, 2009. This survey included additional questions designed to obtain a better understanding of the results from industry's critical asset identification process. In general, this survey did not demonstrate a significant increase in identified critical assets. NERC noted some encouraging results as well as some that were a cause for concern. In addition, the Regional Entities have been performing audits which have included registered entities' determination of their critical cyber asset lists. FERC staff has been observing selected audits to examine the Regional Entities' methods of conducting these audits. It is important to note that although "critical assets" are used to identify subsequent "critical cyber assets," only the subset of "critical cyber assets" are subject to the CIP standards.

NERC's Critical Infrastructure Protection Committee released a guidance document to assist registered entities in identifying their critical assets. That document, which took effect on September 17, 2009, provides "guidelines" that define which assets should be evaluated, provides risk-based evaluation guidance for determining critical assets, and describes reasonable bases that could be used to support that determination. A second NERC security guideline regarding critical cyber assets became effective on June 17, 2010. This security guideline "provides guidance for identifying Critical Cyber Assets by evaluating potential impacts to 'reliable operation' of a Critical Asset." Neither of these guidance documents contained any actions that were mandatory for users, owners or operators of the bulk-power system.

Version 4 of the CIP standards, which are currently pending before the Commission, would change the way in which critical assets are identified. Instead of using a loosely defined risk-based assessment methodology, CIP-002 Version 4 Attachment 1 contains what NERC describes as "uniform criteria for the identification of Critical Assets." For example, criterion 1.1 would identify generation plants equal to or greater than 1500MW as critical assets. The filing asserts that this would account for 29% of the installed generator capacity in the United States. Because this is an on-going proceeding before the Commission, I am limited in what I can discuss about the merits of NERC's petition.

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 CIP standards approved by the Commission in January 2008 took approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for stakeholder 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. 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.

The procedures used by NERC are appropriate for developing and approving routine 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. On September 3, 2010, FERC approved a new reliability standards process manual filed by NERC. While this manual includes a process for developing a standard related to a confidential issue, the new process is untested and it is unclear how the process would be implemented.

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, could 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 directly 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.

This concern was highlighted in the Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security." The audit report identified concerns regarding the adequacy of the CIP standards and the implementation and schedule for the CIP standards, and concluded that these problems exist, in part, because the Commission's authority to ensure adequate cyber security over the bulk electric system is limited. The audit report concludes that the Commission should take a more aggressive action when ordering new or revised standards and highlights its lack of authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities. This report emphasizes the need for FERC to have additional authority for ensuring adequate cyber security over the bulk electric system.

Finally, the open and inclusive process required for standards development is not consistent with the need to protect security-sensitive information. For instance, a formal request for a new standard 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 Formal Notices

Currently, the alternative to a mandatory reliability standard is for NERC to issue a formal notice encouraging utilities and others to take voluntary action to guard against a specific cyber or other vulnerability. Such a notice may be an Advisory, a Recommendation or an Essential Action. The notice approach allows for quicker action, but compliance with a notice is voluntary, and will likely produce inconsistent and potentially ineffective responses. For example, two Advisories and a Recommendation were issued in 2010 by NERC, regarding an identified cyber security threat referred to as "Stuxnet." The details of actions taken to mitigate the vulnerabilities identified by Stuxnet, and the assets to which they apply, as well as their effectiveness, are not known. Reliance on voluntary measures to protect national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards are not sufficient to protect the reliability of the bulk power system.

Smart Grid

The need for vigilance will 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 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 and must be assured before widespread installation of new equipment. 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.

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.

In addition to any smart grid related standards that may be adopted by the Commission, the CIP standards will apply to some, but not most, 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 should be considered a critical cyber asset subject to the protection requirements of the CIP standards. However, this designation is currently up to the affected entity as part of its self-determination of critical cyber assets, as discussed previously.

Many of the smart grid applications will be deployed at the distribution and end-user level. 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.

Physical Security And Other Threats To Reliability

The existing reliability standards do 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 EMP 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.[2] Both electrical equipment and control systems can be damaged by 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 semiconductor technology did not exist 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."[3] 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. The power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced currents. The damage or destruction of numerous transformers across the country would result in reduced grid functionality and 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] Dr. John S., Jr. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (2008).

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

In March 2010, Oak Ridge National Laboratory (Oak Ridge) and their subcontractor Metatech released a study that explored the vulnerability of the electric grid to EMP-related events. This study was a joint effort contracted by FERC staff, the Department of Energy and the Department of Homeland Security and expanded on the information developed in other initiatives, including the EMP commission reports. The series of reports provided detailed technical background and outlined which sections of the power grid are most vulnerable, what equipment would be affected, and what damage could result. Protection concepts for each threat and additional methods for remediation were also included along with suggestions for mitigation. The results of the study support the general conclusion that EMP events pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

The existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure.

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 physical threats to the bulk power system that pose national security concerns.

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 my opinion, the cyber security discussion draft addresses this concern by allowing the Commission to timely act on cyber security vulnerabilities before an incident occurs and by giving the Secretary of Energy emergency authority to act on cyber security threats. In particular, the Commission should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action.

Second, any legislation should allow the Commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack and the Commission will not be able to adequately protect it. The cyber security discussion draft also includes provisions for protection of critical electric infrastructure information, which includes a provision for FERC to establish procedures to allow the Commission to release critical infrastructure information to the extent necessary to enable entities to implement any FERC order under the proposal. It also appropriately would require FERC to limit redistribution of information so that the information is only in the hands of those that need to know.

Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize Commission action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas. The cyber security discussion draft would apply to any entity that owns, controls, or operates critical electric infrastructure. While Alaska and Hawaii would be excluded, the discussion draft requires the Secretary of Defense to prepare a comprehensive plan to protect any national defense facilities located in those states.

Fourth, it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats. The cyber security discussion draft requires the Commission to permit public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary of Energy to avert or mitigate a cyber security threat. I support this provision and any clarifications that might better ensure recovery of costs incurred under this legislation.

Finally, in my view, any legislation on national security threats to reliability should address not only cyber security threats but also natural events; i.e., a geomagnetic disturbance, or intentional physical malicious acts (targeting, for example, critical substations and generating stations) including threats from an electromagnetic pulse. 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.

In short, any new authority should allow the Commission to quickly order mandatory measures that are focused and confidential to address fast-moving, sophisticated and targeted cyber and physical attacks and natural events while providing cost recovery to the affected entities.

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. The cyber security discussion draft in front of us today would go a long way to resolving this issue. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.