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
September 12, 2012

Mr. Chairman, Ranking Member 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.

The Commission is committed to protecting the reliability of the nation's bulk electric system. The Commission is considering actions that it can take under its current authority to address national security threats to the reliability of our transmission and power system from electromagnetic pulses. 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. I will describe how limitations in Federal authority may not fully protect the grid against security threats due to electromagnetic pulse and summarize the Commission's oversight of the electric grid under section 215 of the Federal Power Act.

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 author or 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 under section 215 is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. It also excludes all local distribution facilities, including those facilities connected to defense infrastructure. The current interpretation of "bulk power system" also excludes some transmission, 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 directed 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 has recently filed a revised definition of the term bulk power system, and the Commission has solicited comments on its proposal to accept NERC's revised definition. 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, including those connected to defense infrastructure.

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. However, the NERC process typically requires years to develop standards for the Commission's review.

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 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 to develop a new or modified Reliability Standard using an expedited reliability standard development process 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 expedited process. In the meantime, the bulk power system would be left vulnerable to a known national security threat. Moreover, existing procedures, including the expedited action procedure, could widely publicize both the vulnerability and the proposed solution, 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.

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.

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. While the Commission is considering actions that it can take under its current authority, this authority may not be sufficient in cases where quick mandatory action is needed to protect the United States from the EMP threat or other national security threats to the reliability of our transmission and power system. The Federal government should have no less ability to act to protect against potential damage from physical threats to the grid than from cyber attacks.

One example of a physical threat is an electromagnetic pulse (EMP) event. EMP events can be generated from either naturally occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents on the electric grid. This effect, also termed the "E3" component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area. Regarding man-made events, EMP can also be generated by weapons. Equipment and plans are readily available that have the capability to generate high-energy bursts, termed "E1", that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets. The most comprehensive man-made EMP threat is from a high-altitude nuclear explosion. It would affect an area defined by the "line-of-sight" from the point of detonation. The higher the detonation the larger the area affected, and the more powerful the explosion the stronger the EMP emitted. The first component of the resulting pulse E1 occurs within a fraction of a second and can destroy control and communication electronics. The second component is termed "E2" and is similar to lightning, which is well-known and mitigated by industry. Toward the end of an EMP event, the third element, E3, occurs. This causes the same effect as solar magnetic disturbances. It can damage or destroy power transformers connected to long transmission lines and cause voltage problems and instability on the electric grid, which can lead to wide-area blackouts. It is important to note that effective mitigation against solar magnetic disturbances and non-nuclear EMP weaponry provides effective mitigation against a high-altitude nuclear explosion.

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

[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).

that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] The reports concluded that both electrical equipment and control systems can be damaged by EMP. The reports also pointed out how the interdependencies among the various infrastructures could become vulnerabilities after an EMP. In particular, they point to the electrical infrastructure's need of the communication and natural gas infrastructures.

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.

In March 2010, Oak Ridge National Laboratory (Oak Ridge) and its 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.

In February 2012, NERC released its Interim Report: Effects of Geomagnetic

---

[2] Dr. John S. Foster, 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).

Disturbances on the Bulk Power System. In it, NERC concluded that the most likely worst-case system impact from a severe geomagnetic disturbance is voltage instability and voltage collapse with limited equipment damage.

On April 30, 2012, the Commission held a technical conference to discuss issues related to reliability of the bulk power system as affected by geomagnetic disturbances. The conference explored the risks and impacts from geomagnetically induced currents to transformers and other equipment on the bulk power system, as well as options for addressing or mitigating the risks and impacts. The Commission is considering the comments filed after that conference and what actions it can take under its current authority to address national security threats to the reliability of our transmission and power system from electromagnetic pulses.

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.

Conclusion

Although the Commission's current authority allows it to require the submission by the ERO of proposed standards to address the EMP threat to the United States, it does not allow the Commission the ability to author the standard, thereby limiting its effectiveness. The Commission is considering actions that it can take under its current authority. This authority, however, does not allow it to author standards or to require quick action to protect the United States from the EMP threat or other national security threats to the reliability of our transmission and power system. Any new legislation should address several key concerns, including allowing the federal government to take action before a cyber or physical national security incident has occurred, ensuring appropriate confidentiality of sensitive information submitted, developed or issued under new authority, and allowing cost recovery for costs entities incur to mitigate vulnerabilities and threats.

These types of threats pose an increasing risk to the power grid that serves our Nation, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.