Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation
Before
The Energy and Power Subcommittee of the House Energy and Commerce Committee

Hearing on Discussion Draft Legislation to Improve Cybersecurity of the Electric Grid

May 31, 2011

Introduction

Good afternoon Chairman Whitfield, Ranking Member Rush, members of the Committee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have more than 30 years' experience in the bulk power system[1] industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program. I appreciate the opportunity to testify today on the discussion draft of electric grid cybersecurity legislation.

NERC's Mission

NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system. NERC is an independent corporation whose membership includes large and small electricity consumers, government representatives, municipalities, cooperatives, independent power producers, investor-owned utilities, independent transmission system operators and federal power marketing agencies such as TVA and Bonneville

[1] The Bulk Power System (sometimes referred to as "BPS") is defined in Section 215(a)(1) of the Federal Power Act ("FPA") as: "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof): and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy."

Power Administration. Because the electric grid spans the U.S.-Canada border, NERC's membership includes a number of Canadian entities.

In 2007, NERC was certified as the Electric Reliability Organization (ERO) within the United States by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. Upon approval by FERC, NERC's reliability standards became mandatory within the United States. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by mankind. Throughout North America, four interconnections with a capacity of over one-million megawatts of generation and nearly half-a-million miles of high voltage transmission lines all acting in unison, meet the electric needs of more than 340 million people, with a maximum demand of nearly 850 thousand megawatts. The electricity being used in this room right now is generated and transmitted in real time over a complex series of lines and stations from as far away as Ontario or Tennessee. As complex as it is, few machines are as robust as the bulk power system. Decades of experience with hurricanes, ice storms and other natural disasters, as well as mechanical breakdowns, vandalism and sabotage, have taught the electric

industry how to build strong and reliable networks that generally withstand all but the worst natural and physical disasters while supporting affordable electric service. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electric industry culture of reliability, affecting how it plans, operates and protects the bulk power system.

The Cybersecurity Challenge for the Grid and NERC's Approach to Addressing It

Along with the rest of our economy, the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the reliability of the bulk power system. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the bulk power system requires constant vigilance and expertise.

As CEO of the organization charged with overseeing the reliability and security of the North American grid, I am deeply concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks where we are left to imagine scenarios that might occur and prepare to avoid or mitigate the consequences. Some of those consequences could be much more severe than we have previously experienced. I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature.

The most effective approach against such adversaries is through thoughtful application of resiliency principles, as outlined in a National Infrastructure Advisory Council (NIAC) report on the grid delivered to the White House in October 2010. I served on that council along with a number of industry CEOs. Resiliency requires proactive readiness for whatever may come our way and includes

robustness; the ability to minimize consequences in real-time; the ability to restore essential services; and the ability to adapt and learn. The NIAC's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved sharing of actionable information by government regarding threats and vulnerabilities; 3) cost recovery for security investments driven by national policy; and 4) a strategy on spare equipment with long lead times, such as electric power transformers.

The Administration's recently issued cybersecurity proposals are consistent with these resiliency principles. NERC supports the Administration's comprehensive approach, particularly its emphasis on public-private partnerships and consensus measures to enhance the cybersecurity of all critical infrastructures.

Critical Infrastructure Protection ("CIP") Reliability Standards and other NERC Measures to Address Cybersecurity Threats and Vulnerabilities

1. Reliability Standards

In the Energy Policy Act of 2005, Congress expressly defined the reliability standards to be developed by the ERO and approved by FERC as "including cybersecurity protection …." Sec. 215(a)(3). NERC has nine existing CIP standards that address the following areas:

• Standard CIP-001: Covers Sabotage Reporting.

• Standard CIP-002: Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

• Standard CIP-003: Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

• Standard CIP-004: Requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

• Standard CIP-005: Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

• Standard CIP-006: Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

• Standard CIP-007: Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

• Standard CIP-008: Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

• Standard CIP-009: Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

In December 2010, NERC approved an enhancement to its Critical Cyber Asset Identification standard (CIP-002 version 4) that establishes bright-line criteria for the identification of critical assets. This enhanced standard was filed with FERC in February 2011 and is currently pending FERC approval.

Compliance with the NERC CIP standards is an important threshold for properly securing the BPS. However, there is no single security asset, security technique, security procedure or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best-practices call for additional processes, procedures and technologies beyond those required by the CIP standards.

Since it became the ERO, NERC, working with FERC, has developed mechanisms to promulgate standards on an expedited and/or confidential basis if necessary to address imminent or longer term national security threats. In addition, FERC can order NERC to develop a reliability

standard or a modification to a reliability standard to address a specific matter (such as a cyber threat or vulnerability) under FPA Section 215(d)(5)[2] Finally, the NERC Board of Trustees may propose and adopt a standard in response to a FERC directive if the board determines that the regular standards process is not being sufficiently responsive to the Commission.

2. NERC Alerts

Not all vulnerabilities can or should be addressed through a reliability standard. In such cases, NERC Alerts are a key element in critical infrastructure protection. To address cyber challenges not covered under the CIP Standards, NERC works through its Electricity Sector-Information Sharing and Analysis Center (ES-ISAC) to inform the industry and recommend preventative actions.

NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies, including the Department of Homeland Security and the Department of Energy National Laboratories, and bulk power system subject matter experts, called the HYDRA team, to communicate sensitive information to the industry. As defined in NERC's Rules of Procedure, the ES-ISAC developed the following three levels of Alerts for formal notice to industry regarding security issues:

• **Industry Advisory** - Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.

• **Recommendation to Industry** - Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the Alert.

[2] "Section 215(d)(5) of the FPA authorizes the Commission to direct the ERO to submit to the Commission a new or modified Reliability Standard that addresses a specific matter if the Commission considers the new or modified Standard appropriate to carry out section 215." *Order Denying Rehearing, Denying Clarification, Denying Reconsideration, and Denying Request for Stay re North American Electric Reliability Corporation*, 132 FERC ¶ 62,218 (2010).

• **Essential Action** - Identifies actions deemed to be "essential" to bulk power system reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the Alert.

The risk to the bulk power system determines selection of the appropriate Alert notification level. Generally, NERC distributes Alerts broadly to some 1900 users, owners, and operators of the bulk power system in North America, utilizing its Compliance Registry. NERC also distributes Alerts to other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g.; Balancing Authorities, Planning Authorities, Generation Owners, etc.).

NERC has issued 14 CIP-related Alerts since January 2010 (12 Industry Advisories and two Recommendations to Industry). Those Alerts covered items such as Aurora, Stuxnet, Night Dragon and the reporting of suspicious activity. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders. In addition, NERC released one Joint Product CIP Awareness Bulletin in collaboration with DOE, DHS and the FBI titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)".

The NERC Alert system is working well. It is known by industry, handles confidential information and does so in an expedited manner. An Alert does not require a NERC balloting process, but it is not enforceable as reliability standards are.

NERC Works with DOD, DHS and DOE to Protect Grid Cybersecurity

As chair of the Electricity Sub-Sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the government, including the Department of Defense, the Department of Homeland Security and the Department of Energy, to discuss and identify critical infrastructure protection concepts, processes and resources, as well as to facilitate information sharing about cyber

vulnerabilities and threats. This type of public/private partnership is key to effective cybersecurity protection.

Recently, I met with officials from U.S. NORTHCOM where we discussed collaborating on various electric grid-focused activities including participation in the 2011 SecureGrid Exercise, providing electric sector situational awareness and collaborating on the Joint Capability Technology Demonstration (JCTD) Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). The latter project is being proposed to understand how specific facilities could develop small reliable "micro-grids" on a short-term or emergency basis.

NERC is working with DHS National Cybersecurity and Communications Integration Center to develop a Memorandum of Understanding for bi-directional sharing of critical infrastructure protection information between the government and the electricity sector in North America. NERC also provides leadership to two significant DHS-affiliated public-private partnerships. These are the Partnership for Critical Infrastructure Security (PCIS) and the Industrial Control Systems Joint Working Group (ICSJWG). The PCIS is the senior-most policy coordination group between public and private sector organizations. On the government side, PCIS comprises the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating Councils. On the private side, PCIS comprises the chairs of all of the private-sector coordinating councils. The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC is engaged with DOE National Laboratories to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the bulk power system. We are working with Pacific Northwest National Laboratory on the Electric Sector Network Monitoring

initiative and also on developing cybersecurity certification guidelines for Smart-Grid Cyber Operators. In a similar fashion, NERC is working with the Idaho National Laboratory to promote the Cyber Security Evaluation Tool for use within the electric sector. NERC also is partnering with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability and security incident information.

Finally, NERC is working with DOE and the National Institute of Standards and Technology to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including both the bulk power system and distribution systems. We believe this to be particularly important with the increasing availability of smart-grid and smart-meter technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the bulk power system. Everyone engaged in smart-grid and smart-meter implementation should ensure that appropriate security applications and technologies are built into the system to prevent the creation of additional threats and vulnerabilities.

NERC Comments on the Discussion Draft

1. **Government authority to deal with cyber emergencies is needed.**

NERC has consistently supported comprehensive legislation authorizing some government entity to address cyber emergencies. Which agency is a policy decision for Congress to make; the current draft would give the Commission that authority, upon a determination by the President identifying an imminent grid security threat. Whatever approach is chosen, NERC stands ready to assist in responding to identified grid security threats.

2. **Measures to improve information sharing between the government and private sector owners of critical grid infrastructure are also needed.**

NERC strongly supports efforts to improve information sharing between government and the private sector owners of critical electric infrastructure. NERC especially commends the provisions of

the discussion draft directing the Commission to facilitate the appropriate sharing of protected information between and among government entities and those in the private sector who are subject to the proposed legislation.

NERC and the electric industry can only deal with the risks they are aware of. It is impractical, inefficient and impossible to defend against all possible threats or vulnerabilities. Entities must prioritize their resources to protect against those risks that pose the greatest harm to their assets and their customers. The electric industry best understands the impact that a particular event or incident could have on the bulk power system, but the industry does not have the same access to actionable intelligence and analysis that the government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and vulnerabilities. Too often the industry has heard from government agencies that the threats are real, but is given little or no additional information. This leads to frustration among the private sector entities that are unable to respond effectively due to ill-defined and nebulous threat information.

NERC appreciates the attention in the discussion draft to providing adequate security clearances to key industry personnel, but this alone cannot effectively address the unavailability of actionable information for electricity industry decision-makers. NERC has over 1900 entities on its Compliance Registry; some have just a few employees and some have many thousands. Given the necessarily limited number of security clearances that may be made available, it is more important to develop methods for declassifying sensitive information so that key data can be made available to the broad range of industry decision-makers who must act to protect the grid against the threat or vulnerability.

3. Additional authority to address Grid Security Vulnerabilities is not necessary.

As discussed above, NERC has the existing tools, the expertise and the relationships with government agencies, intelligence resources and industry subject matter experts to address identified

vulnerabilities effectively and efficiently. In addition, FERC has the authority under FPA Sec. 215(d)(5) to direct NERC to prepare a standard to address a specific vulnerability or other matter, and to do so by a certain date, if FERC decides the matter needs that level of priority. Thus, it is not clear to NERC that the vulnerability section (proposed new FPA Section 215A(c)) is needed.

If Congress decides to address vulnerabilities through a FERC order, at a minimum, the ERO should be given the opportunity to address the vulnerability identified by FERC within a time certain, similar to the current authority under Sec. 215(d)(5).

With respect to the existing cybersecurity vulnerability addressed in proposed Section 215A(c)(2) of the discussion draft, the industry now understands the Aurora vulnerability and is mitigating that vulnerability. Therefore, NERC believes section 215A(c)(2) is not needed. From 2007 through 2010, NERC worked closely with federal partners on information controls and was finally authorized to share with industry an extensive technical library through NERC's protected portals. The availability of this technical library allowed NERC, federal partners, and industry subject matter experts to develop and issue an Aurora "Recommendation to Industry" Alert on October 13, 2010 with explicit information on the vulnerability and recommendations for detailed mitigation measures. More importantly, the availability of the technical library allowed the asset owners to assess for themselves the true nature of the Aurora vulnerability and begin to devise mitigations to address that vulnerability. This NERC Level 2 "Recommendation to Industry" carried mandatory reporting obligations in accordance with NERC Rules of Procedure (ROP)[3] and NERC continues to work with industry on mitigation efforts. Over the past three weeks, NERC has held Aurora mitigation webinars attended by over 800 industry subject matter experts.

[3] Section 810, *Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions.*

4. ERO Authority to Address Grid Security Vulnerabilities by enforceable means other than Reliability Standards would be useful.

Not all Grid Security Vulnerabilities can or should be addressed by a reliability standard. Currently, however, NERC actions other than reliability standards are not legally enforceable. Legislation authorizing NERC to promulgate legally enforceable directives in response to the Commission's identification of a Grid Security Vulnerability and a Commission order to NERC to address that vulnerability could enhance the cybersecurity of the grid. In order to be enforceable, such an ERO directive would need to be approved by the Commission.

5. Geomagnetic Storms and Spare Transformer provisions are not needed.

Section 215A(c)(4) and (c)(5) of the discussion draft address, respectively, geomagnetic storms and large transformers. NERC is currently working with two separate task forces to address geomagnetic storms and spare transformer issues. NERC's Geomagnetic Disturbance ("GMD") Task Force recently held a workshop focused on potential mitigation approaches and issued an Industry Advisory NERC Alert on GMD[4]. This Alert provides industry with guidance to prepare for the effects of severe GMD on the bulk power system.

With respect to spare transformers, in September 2010, NERC initiated the Spare Equipment Database (SED) Task Force to redesign and update the policies and protocols for the use of this Database across North America. This effort is also designed to obtain broader participation by bulk power system owners and expanded information on spare transformers. In conjunction with EEI's Spare Transformer Equipment Program, and the many pooling/bilateral agreements that exist today among industry participants, NERC's SED program will support utilities in responding to and managing bulk power system reliability in the event of an event that causes loss of transformers.

[4] http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01_GMD_FINAL.pdf

Currently, FERC can order NERC to address either one of these topics under Sec. 215(d)(5). Consequently, these legislative provisions in the discussion draft are not needed. If Congress chooses to direct action on these topics as a high priority, however, NERC supports the language in the discussion draft that requires FERC to specify the nature and magnitude of the reasonably foreseeable events or attacks against which reliability standards must protect (in the case of geomagnetic storms) or which provide the basis of the standards (in the case of large transformer availability). NERC also supports the provisions in the discussion draft requiring that such standards appropriately balance the risks associated with a reasonably foreseeable attack or event, including any regional variation in such risks, with the costs of mitigating such risks.

Conclusion

NERC works with multiple agencies, industry, consumers and government to support a coordinated comprehensive effort to address cybersecurity. As outlined today, NERC has many tools available including the ESCC and the ES-ISAC to address immin**e**nt and non-imminent threats and vulnerabilities through its Alerts and reliability standards processes in a timely, efficient and effective manner. These existing processes should be enhanced, not pre-empted, by cybersecurity grid legislation.

We appreciate this opportunity to discuss NERC's activities on cybersecurity with the subcommittee and to offer our views on legislation that would improve cybersecurity protection of the grid.