Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation
Senate Energy and Natural Resources Committee
Hearing to receive testimony on a joint staff Discussion Draft pertaining to cybersecurity of the bulk-power system and electric infrastructure

May 5, 2011

Introduction

Good morning Chairman Bingaman, Ranking Member Murkowski, 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 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,

[1] The Bulk Power System (sometimes referred to as "BPS") is defined as generation and transmission of electricity greater than 100kv, in contrast to the distribution of electricity to homes and businesses at lower voltages.

municipalities, cooperatives, independent power producers, investor-owned utilities, independent transmission system operators and federal power marketing agencies such as TVA and Bonneville Power Administration.

In 2007, NERC was designated the Electric Reliability Organization (ERO) 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 and approved by FERC, 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. Examples of the NIAC team'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.

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

NERC's critical infrastructure program, including both reliability standards and alerts, provides many tools to respond to cyber threats and vulnerabilities. Industry, consumers, and government representatives all participate in the NERC standards development process and provide important expertise.

1. Reliability Standards

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.

In addition to the development of reliability standards through NERC's regular processes, FERC has authorized NERC to use an expedited standards development process to meet urgent reliability issues. NERC also has rules approved by FERC to enable the development of special standards on an expedited, confidential basis to address imminent or longer term national security threats.

Finally, FERC can order NERC to develop a proposed 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). In addition, 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.

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.

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 must be able to promptly disseminate threat indications, analyses and warnings to assist electricity-sector participants in taking protective actions. NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies to communicate sanitized 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.
- **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 users, owners, and operators of the bulk power system in North America utilizing its Compliance Registry. Entities registered with NERC are required to provide and maintain up-to-date compliance and cyber security contacts. NERC also distributes the Alerts beyond the users, owners and operators of the bulk power system, to include 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.)

Alerts are developed with the strong partnership of Federal technical organizations, including the Department of Homeland Security and the Department of Energy National Laboratories, and bulk power system subject matter experts, called the HYDRA team by NERC. 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. The information needed to develop the Alert is managed in a confidential and expedited manner and does not require a NERC balloting process.

NERC understands that the Congress is seeking to ensure the cybersecurity of the electricity grid. Using standards, Alerts and essential actions, NERC is already working with FERC and the industry to protect the cybersecurity of the bulk power system.

NERC Work 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. Similarly, NERC is discussing a project with DOD to develop case studies at critical military installations to further understand the requirements for "flow of power" and the implications to military readiness.

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

First and foremost, NERC has consistently supported legislation authorizing some government entity to address cyber emergencies, as the draft would authorize the Secretary of Energy to do.

Second, NERC strongly supports any effort 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 Secretary and the Commission to establish procedures on the release of critical infrastructure information to entities 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 ensure they are protected against those risks that pose the greatest harm to their assets, their business and their customers. The electric industry is in the best position to understand 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 leaders who are unable to respond effectively due to ill-defined and nebulous threat information.

NERC also appreciates the additional attention in the discussion draft to providing security clearances, but that route will not likely deal with 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. It is important to be realistic about the number of clearances that may be made available. Of more importance is developing methods and procedures for sanitizing sensitive information so that it can usefully be made available to the broad range of private decision-makers who must take action to protect against the threat or vulnerability.

The bulk of NERC's comments are directed to the draft legislation's treatment of "Cyber Security Vulnerabilities," which are something less urgent than "Cyber Security Threats." NERC appreciates that the draft legislation proposes for the ERO to play a meaningful role in addressing cybersecurity vulnerabilities, as the ERO now does. As discussed above, NERC has the tools, the expertise and the relationships with government agencies, intelligence resources and industry subject matter experts to address identified vulnerabilities effectively and efficiently. FERC has the authority now under FPA Sec. 215(d)(5) to direct NERC to prepare a proposed standard to address a specific vulnerability or other matter, and to do so by a certain date. Thus, it is not clear to NERC that the vulnerability section (proposed new FPA Section 224(b)) is needed. If this section is retained, please consider the following concerns:

1. **FERC's jurisdiction under this bill extends to distribution systems; the ERO's does not:** The definition of Critical Electric Infrastructure in proposed Section 224 extends to distribution systems. Section 215 does not provide NERC with that jurisdiction. Thus, existing NERC reliability standards and requirements cannot be as broad as FERC's jurisdiction under the draft bill, and standards prepared by NERC at the direction of FERC similarly cannot be as broad as FERC's direction if FERC directs an action to protect the distribution system action. If NERC is intended to have the same jurisdiction as FERC over the distribution system and assets, this needs to be clarified. Without such clarification, FERC could always find that an ERO-proposed reliability standard "fails to provide adequate protection of critical electric infrastructure from a cybersecurity vulnerability" and reject the ERO's efforts under Section 224, effectively removing the ERO role from the vulnerabilities section.
2. **Identification of vulnerability:** No requirement exists in the legislation for FERC to identify any deficiency in existing reliability standards or the specific cybersecurity vulnerability for the ERO to address. Without some idea of the "target" that FERC would like the ERO to hit, it will be difficult for the ERO to produce an adequate set of requirements, assuming the jurisdiction issue above is addressed.
3. **Enforceable tools in addition to standards:** The discussion draft calls for the ERO to develop a reliability standard in response to a FERC order on vulnerabilities, but given the constantly changing nature of vulnerabilities, not all vulnerabilities can or should be addressed by a standard. Currently, NERC actions other than standards are not legally enforceable. Legislation that provides a means for both standards and other NERC directives to be legally enforceable would significantly enhance the cybersecurity of the

grid. Such an approach would require the involvement of both the ERO and the Commission.

4. **Due process:** The discussion draft would authorize FERC to promulgate an interim final rule without consultation or any due process. In addition, unlike the 90-day sunset on DOE emergency orders, there is no such limitation on FERC interim final rules.

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 imminent and non-imminent threats and vulnerabilities through our Alerts and standards processes. 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 committee and to offer our views on legislation that would improve cybersecurity protection of the grid.