Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation
Before the
Senate Energy and Natural Resources Committee
Hearing on the Status of Actions Taken to Ensure that the Electric Grid is Protected from Cyber Attacks

July 17, 2012

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). 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. NERC's reliability standards are mandatory and enforceable within the US for the bulk power system and include Critical Infrastructure Protection (CIP) Standards. 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. NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence with accountability for standards and compliance, risks to reliability and continued coordination and collaboration with public and private sector partners. I testified on this subject before this Committee in May 2011, and I appreciate the opportunity to update the Committee on NERC's activities related to cybersecurity. These activities include, but are not limited to:

1. Receiving FERC approval of NERC's Critical Cyber Asset Identification standards (CIP-002 version 4);

2. Beginning work on a comprehensive revision to the cybersecurity standards, leveraging lessons learned from previous versions;
3. Issuing eight additional alerts related to cybersecurity concerns;
4. Developing a risk management process guideline to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks;
5. Completing the first phase of the High-Impact Low-Frequency Task Force reports identifying recommendations for owners and operators with respect to addressing severe impact resilience, cyber attacks, spare equipment, and geomagnetic disruptions;
6. Facilitating the first-ever Grid Security Exercise (GridEx) for the Electricity Sub-sector in North America; and
7. Participating in government partnership initiatives, including the Department of Homeland Security's (DHS) National Level Exercise series and various cybersecurity forums and briefings with Canadian government agencies, as well as the White House–initiated, Department of Energy (DOE)-led Electricity Sub-sector Cybersecurity Risk Management Maturity Model, which will support ongoing development and measurement of cybersecurity capabilities within the sub-sector;

The Cybersecurity Challenge for the Grid

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. As CEO of the organization charged with ensuring the reliability and security of the North American grid, I remain 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.

To explore the impacts of this changing risk landscape from the view of the newer emerging risks, NERC has worked with industry and government to better understand cybersecurity risks and manage those risks. Based on all of the work NERC has been involved in to date, it is clear that the most effective approach against adversaries exploiting the newer risk landscape is through thoughtful application of resiliency principles. 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.

NERC Measures to Address Cybersecurity Threats and Vulnerabilities

NERC has incorporated these resiliency elements in our strategic approach to ensuring reliability of the bulk power system. This strategic approach includes: 1) developing mandatory and enforceable standards; 2) ensuring compliance and audit oversight; 3) sharing and analyzing information and issuing Alerts from the Electricity Sector Information Sharing and Analysis Center (ES-ISAC); 4) engaging in private-public partnerships; and 5) conducting outreach,

training, and education activities within and external to the bulk power system. Only through these critical infrastructure protection components can we achieve a balanced approach to guard against advanced persistent threats to grid cybersecurity and mitigate vulnerabilities.

Reliability Standards

In 2007, FERC designated NERC the ERO in accordance with Section 215 of the Federal Power Act, enacted by the Energy Policy Act of 2005. Upon FERC's approval, NERC's reliability standards became mandatory within the US. These mandatory reliability standards include 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 US. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid.

NERC's nine mandatory CIP standards 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 with access 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: Addresses 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 the Federal Energy Regulatory Commission (FERC) in February 2011, and FERC approved the standard on April 19, 2012. The implementation of the CIP standards under the bright-line approach is currently underway.

In addition, industry is currently developing a comprehensive revision to the cybersecurity Standards. The revision leverages experience with existing CIP standards to enhance the industry's protections against cyber threats and vulnerabilities, including transitioning the classification of critical assets to a "low-medium-high" impact-based system. The revised CIP standards will also provide greater flexibility in implementing solutions to emerging cyber threats. The revised CIP standards have been improved to remove technology-specific requirements by replacing them with a risk-based approach to implementing appropriate and changing technologies. That is, rather than specifying how to implement a requirement, the revised requirements specify the risk-based result that must be achieved, which enables industry to implement new and emerging technologies to address the risk.

NERC can use an emergency standards development process if circumstances warrant. In addition, FERC can order NERC to develop or modify a reliability standard to address a specific matter.[1] Finally, the NERC Board of Trustees can direct NERC to develop and adopt a standard in response to a FERC directive and timetable if the Board determines that the regular standards process is not sufficiently responsive to the Commission.

Under the emergency standards process, FERC has authorized NERC to use an expedited standards development process to meet urgent reliability issues. These special standards can be developed on an expedited, confidential basis to address imminent or longer-term national

[1] 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).

security threats. NERC has practiced using this expedited, confidential process as part of GridEx.

In addition to developing mandatory reliability standards, NERC supports the ERO's Regional Entities to improve the consistency of compliance program results, improve risk-based approaches for auditing and spot checking, and promote a culture of security and compliance through education, transparency, and incentives. Specifically, we conduct audit oversight of the Regional Entities' compliance audit teams during audits of registered entities, and maintain oversight throughout the entire audit process (pre-audit, on-site, and post audit) in accordance with the audit oversight program. During this process, NERC seeks to capture compliance applications, positive observations, lessons learned, and recommendations. NERC's audit oversights are designed to perform a thorough evaluation of the processes and criteria used by all Regional Entities in their determination of registered entities' compliance with the NERC Reliability Standards, including the CIP Standards.

Compliance with the NERC CIP standards is an important threshold for properly securing the bulk electric system. However, no single security asset, technique, procedure, or standard—even if strictly followed—will protect an entity from all potential cyber 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.

The ES-ISAC and 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 ES-ISAC to inform the industry and recommend mitigation actions.

The ES-ISAC gathers information from disparate electric industry participants about security-related events, disturbances, and off-normal occurrences within the Electricity Sub-sector and shares that information with key governmental entities. In turn, these governmental entities provide the ES-ISAC with information regarding risks, threats, and warnings which the ES-ISAC is then responsible for disseminating throughout the Electricity Sub-sector. The two functions that the ES-ISAC supports, information sharing and analytics, are vitally important to all other critical infrastructures and key resource sectors that have active ISACs. Effective collaboration and communication is essential to addressing infrastructure protection and resilience within each sector, as well as the important interdependencies that exist among sectors.

NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies to communicate unclassified 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, Transmission Operators, Generation Owners, etc.).

Alerts are developed with the strong partnership of Federal technical organizations, including DHS and DOE National Laboratories, and bulk power system subject matter experts, called the HYDRA team. NERC has issued 22 CIP-related Alerts since January 2010 (20 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 Federal Bureau of Investigation (FBI) titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPN)."

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. Information sharing through the ES-ISAC is the greatest asset we have to combat emerging threats to cybersecurity and help ensure the reliability of the bulk power system. As a result, NERC has been enhancing the ES-ISAC's capabilities by building out a private, secure portal to receive voluntary reports from industry members and working with various organizations (both industry and government) to obtain the data and mechanisms necessary to conduct these information sharing activities.

Anything Congress can do to further facilitate information sharing between the public and private sector would add greatly to these efforts. Some actions may include: making more clearances available to industry, identifying alternative methods to communicate classified information to our Canadian partners, and encouraging increased information sharing by US Government departments and agencies with asset-owners.

NERC's Public-Private Partnerships to Enhance Grid Cybersecurity

As mentioned, NERC has developed several strong relationships with industry and government entities. 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,

DOE, and DHS, to identify, discuss, and resolve critical infrastructure protection policy, process, and resource issues. This type of public-private partnership is essential to effective cybersecurity protection by facilitating information sharing about cyber-related vulnerabilities and threats.

Last year, NERC signed a Cooperative Research and Development Agreement with DHS that provides ES-ISAC staff with access to DHS' National Cybersecurity and Communications Integration Center (NCCIC). Access to the classified NCCIC facilitates a significantly improved bi-directional sharing of critical infrastructure protection information between the US government and the Electricity Sub-sector in North America. NERC has also recently established a protected communications corridor for the ES-ISAC in part to facilitate this bi-directional information sharing between the DHS NCCIC and BPS entities.

NERC also provides leadership to three significant DHS-affiliated public-private partnerships. These groups are:

- *Partnership for Critical Infrastructure Security*, the senior-most policy coordination group between public and private sector organizations comprised of the chairs or co-chairs of all 18 critical infrastructure and key resources sectors and their Government Coordinating Council counterparts;
- *Cross-Sector Cyber Security Working Group*, which was established to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services; and
- *Industrial Control Systems Joint Working Group*, which is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector

strategic roadmap development, and coordinated efforts to develop better vendor focus on security needs for industrial control systems.

NERC also collaborates with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

As part of NERC's outreach and awareness efforts to engage industry and government in addressing some of the key cybersecurity challenges we face, NERC facilitated the first-ever Grid Security Exercise (GridEx) for the Electricity Sub-sector in North America. This distributed play exercise, which was held in November 2011, was designed to validate the readiness of the Electricity Sub-sector to respond to a cyber incident, strengthen utilities' crisis response functions, and provide input for internal security program improvements. Seventy-five industry and government organizations from the US and Canada participated in GridEx. BPS entities included generation and transmission owners, reliability coordinators, independent system operators, and balancing authorities. Key government agencies, such as DHS, FBI, and DOE, were also heavily involved. GridEx provided a realistic environment for organizations to assess their cyber response capabilities. The biennial exercise was viewed across industry and government as a training success in preparing the BPS for a disruptive security event. NERC issued a final report in March 2012, and is applying the GridEx recommendations to further strengthen the bulk power system's preparedness and response mechanisms.

Given the heightened awareness of security in the Electricity Sub-sector, NERC hosts an annual Grid Security Conference (GridSecCon) to discuss emerging threats, industry best practices, and

provide cutting edge training to the industry. NERC will again host this conference in October 2012, and will bring together cyber and physical security thought leaders from government and industry to discuss securing industrial control systems, social engineering attacks, and security event response management, among other topics.

Conclusion

As outlined today, NERC has many tools available, including critical infrastructure protection standards and processes and the ES-ISAC, to address immin**e**nt and non-imminent threats and vulnerabilities. We work with multiple government, industry, and consumer partners to support a coordinated comprehensive effort to address cybersecurity.

We appreciate this opportunity to discuss NERC's activities on cybersecurity with the committee related to cybersecurity protection of the grid.