TESTIMONY OF RICHARD P. SERGEL
PRESIDENT AND CHIEF EXECUTIVE OFFICER
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BEFORE THE SUBCOMMITTEE ON ENERGY AND AIR QUALITY
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

Hearing on
PROTECTING THE ELECTRIC GRID FROM CYBERSECURITY THREATS
September 11, 2008

INTRODUCTION

The North American Electric Reliability Corporation (NERC) takes most seriously its responsibilities for protecting the cyber security of the North American bulk power system. Working with our stakeholders, our job is to protect the reliability of the grid, and cyber security is an important element of that responsibility. But the challenges the grid faces from cyber security threats are different from other reliability concerns. Cyber technologies change frequently and potential threats can arise very quickly, requiring rapid, effective and often confidential responses. Threats can arise virtually anytime and anywhere across the vast array of communicating devices on the grid – Supervisory Control and Data Acquisition (SCADA), control rooms, power plants, substations, relays, meters, some transformers, capacitor bank controllers, to name just a few – and the systems to which those devices are connected. Cyber security threats are more likely to be driven by intentional manipulation of devices as opposed to operational events on the bulk power system.

All of these challenges clearly set cyber security apart from other reliability concerns. When there is an identified, immediate threat, a different approach is required

– one that allows for more expedient and confidential treatment of critical information, rapid threat analysis, and directed action on necessary actions. For these reasons, we believe that in the event of an imminent cyber security threat, the U.S. government needs immediate authority to act. With the immediate emergency responsibility in the hands of government, NERC will be better positioned to do its job of developing and implementing cyber security and critical infrastructure protection Reliability Standards that will harden the grid against intrusion and aid in responding effectively to cyber security incidents.

My testimony today will focus on the steps that NERC is taking to enhance protection of the grid from cyber security threats.

I. BACKGROUND

NERC's mission is to ensure that the bulk power system in North America is reliable. To achieve this objective, NERC develops and enforces Reliability Standards that are now mandatory, thanks to the Energy Policy Act of 2005; monitors the bulk power system; assesses and reports on the adequacy of electricity supplies and transmission; and educates, trains and certifies industry personnel. NERC, which draws upon the collective expertise of the electricity industry, is subject to oversight by the Federal Energy Regulatory Commission (FERC) in the United States and by governmental authorities in Canada. FERC certified NERC as the Electric Reliability Organization (ERO) in July 2006.[1] Most Reliability Standards approved by NERC and FERC became mandatory and enforceable in June 2007.

[1] *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

On January 18, 2008, FERC issued Order No. 706, approving eight mandatory Reliability Standards for Critical Infrastructure Protection (CIP Reliability Standards).[2] Approval of the CIP Reliability Standards was a major step forward in ensuring the reliability of the electric grid because these standards set forth specific requirements that are binding on users, owners and operators of the bulk power system to safeguard critical cyber assets. They require identification and documentation of cyber risks and vulnerabilities, establishment of controls to secure critical cyber assets from physical and cyber sabotage, reporting of security incidents, and establishment of plans for recovery in the event of an emergency.

The Critical Infrastructure Protection Reliability Standards approved through Order No. 706 are a sound starting point for the electric industry to address cyber security. Improvement of the CIP Reliability Standards, however, already is underway, both in response to directions given by FERC in Order No. 706 and as part of NERC's ongoing Reliability Standards development process.

II. NEW FEDERAL AUTHORITY TO DEAL WITH CYBER SECURITY EMERGENCIES IS NEEDED

The NERC standards development process is designed to respond to defined, measurable risks that can be identified from operating experience, event analysis, compliance audits, system and equipment performance analysis, and benchmarking programs. The process is structured to leverage industry subject matter expertise against well defined problems with long histories and defined data. This process responds to a need for standards that is transparent, relatively well known and widely understood.

[2] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *reh'g denied,* Order No. 706-A, 123 FERC ¶ 61,174 (2008).

Incremental improvement in standards over time is acceptable for many Reliability Standards.

In contrast, addressing cyber security attacks may require significant change without operating experience as a basis and in very short timeframes. Just as SCADA and communications technologies change frequently, potential threats also arise quickly. Standards relating to critical infrastructure in general, and cyber security in particular, must continue to evolve, but that evolutionary process may not be adequate to respond to an immediate threat. Moreover, the open process by which Reliability Standards are developed, while demonstrably successful in producing standards that have significantly enhanced the reliability of the grid, may not be ideally suited to situations where, because of the sensitive subject matter, confidentiality is required and time does not permit extensive consultation.

The intentional nature of cyber and physical security threats means the protection of the bulk power system is dependent in large measure on the quality and timeliness of threat analysis and risk assessments developed by others outside the electric industry. Classified intelligence information, rather than the observable operating conditions of the bulk power system, can quickly raise the threat level.

NERC draws much of its technical expertise from the collective wisdom of industry volunteers, assembling industry subject matter experts into drafting teams, developing and posting proposed standards for broad industry stakeholder comment, and gaining approval by supermajority vote. For the majority of Reliability Standards, this inclusive process works to elicit the data and information needed for Standards development; however, with respect to cyber security threats, much of the critical

information resides within government agencies and confidential treatment of that information is essential. In non-emergency situations, NERC can coordinate with the appropriate agencies and the limitations associated with confidential information can be managed. Existing authorities and established processes enable both a comprehensive risk assessment and the development of strategies and plans to address those risks to the security of the bulk power system. However, in the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government.

III. NERC'S ROLE IN PROTECTING AGAINST CYBER SECURITY THREATS

NERC reviews cyber security threats on an ongoing basis. NERC's Critical Infrastructure Protection Committee (CIPC),[3] has coordinated NERC's security initiatives for several years. The CIPC Executive Committee, along with the NERC CEO and Chief Security Officer, serve as the Electricity Sector Coordinating Council to collaborate with the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) on critical infrastructure and security matters. Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[4] which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

[3] CIPC is comprised of industry experts in the areas of cyber security, physical security, and operational security. CIPC reports to NERC's Board of Trustees. It is governed by an Executive Committee, whose members manage CIPC policy matters and provide support to CIPC's subcommittees and their working groups and task forces.

[4] The ES-ISAC has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC works with the electricity industry to identify and mitigate cyber vulnerabilities by providing information, recommending mitigation measures, and following up to monitor implementation of recommended measures. NERC, in its capacity as the ES-ISAC, also has some related responsibilities for cyber and physical security issues associated with all electric facilities operated in the United States.

NERC and the industry share a mutual goal to ensure that threats to the reliability of the bulk power system, especially cyber security threats, are clearly understood and are mitigated. NERC in collaboration with the industry is committed to 1) ensuring the reliability of the bulk power system from a cyber security threat; 2) assuring that NERC's efforts will complement those of the government and industry with regard to cyber security protection; and 3) assuring that there are no gaps and that responsibility is clear for execution of cyber security protection initiatives.

NERC has committed to elevating the importance and sense of urgency associated with cyber security threats. Key elements of this strategy are:

Establishment of a Chief Security Officer (CSO) and Creation of a Core NERC Critical Infrastructure Protection Program

Recognizing the critical differences associated with cyber security threats to bulk power system reliability, NERC has consolidated responsibility for coordination of cyber and all other security matters across all NERC activities into a single responsibility area. On September 2, Michael J. Assante joined NERC as "Chief Security Officer." Mr. Assante comes to NERC from the Department of Energy's Idaho National Labs (INL) as a widely recognized expert and visionary in the fields of security and infrastructure protection. He also serves as a member of the Commission on Cyber Security for the 44th Presidency of the United States. Prior to assuming his strategic leadership position at INL, Mr. Assante was a vice president and Chief Security Officer at American Electric Power, one of the largest generators of electric power in the U.S. Mr. Assante thus has the background to lead NERC's cyber security protection program to a new level, and to be a critical point of contact with industry and government. He reports directly to me.

The CSO is responsible for assuring that the Rules of Procedure for all NERC programs are implemented in a timely and effective manner with respect to Critical Infrastructure Protection. He is also responsible for evaluating and recommending any changes to the NERC Rules of Procedure necessary to achieve the objectives of NERC's Critical Infrastructure Protection program. In addition, the CSO is responsible for assuring coordination between NERC and government agencies with respect to all critical infrastructure protection matters, especially where confidentiality is an issue.

As a first step, the CSO, with the assistance of the Regional Entities, will perform an assessment, with metrics and recommendations, of the preparedness of the users, owners, and operators on the NERC compliance registry to address cyber security threats. The assessment and recommendations will address preventing intrusions as well as assessing the capability for isolating and limiting attacks so they remain within our abilities to withstand any subsequent equipment losses and restore the system quickly. The CSO also will represent NERC in the Partnership for Critical Infrastructure Security.

Alternative Standard Setting Process for Cyber Security Standards

NERC has established a task force to review, and where appropriate recommend, a revised standard setting process for cyber security that will include an emergency/crisis standards setting process. This process must provide a level of due process and technical review, but also provide the speed necessary to establish Standards quickly and work seamlessly with any new authority granted in the United States to the FERC. As part of this effort, NERC will investigate and review standards development models from other industries.

Continual Upgrading of Existing CIP Standards

NERC also is working to accelerate the review of the existing CIP Reliability Standards. The Commission in Order No. 706 directed NERC to develop modifications to the CIP Reliability Standards to address specific matters through the Reliability Standards development process. Among other things, NERC is specifically considering the extent to which elements of the Recommended Security Controls for Federal Information Systems under development by the National Institute of Standards and Technology (NIST) can be incorporated into the CIP Reliability Standards. NERC also is developing guidance documents to help entities know what is expected to comply with certain aspects of the CIP Reliability Standards.

Expand Role of Industry Executives at NERC

NERC has formed the Electric Sector Steering Group (ESSG) to provide strategic and policy guidance to the Electricity Sector Coordinating Council and to NERC in its role as the operator of the ES-ISAC. The ESSG includes five CEO-level industry executives, a NERC board member, and the NERC CEO. The five industry executives were selected by NERC's Member Representatives Committee to provide broad stakeholder and geographic representation. Chaired by the NERC CEO, this group will provide high-level policy guidance and broad electricity sector participation and support on critical infrastructure security matters, including matters beyond the bulk power system. This group will be instrumental in providing direction and support for these and future key NERC and industry security initiatives. The ESSG will also provide advice to the CSO as he develops critical infrastructure protection into a core NERC program.

Inclusion of the industry executives will facilitate the peer-to-peer contacts that will be essential to effective implementation of these efforts.

Closer Coordination with Government Stakeholders

NERC, with the guidance of the ESSG, is establishing an enhanced process to conduct comprehensive and continuous assessments of security risks to the bulk power system of North America. Existing risk assessment efforts tend to be focused on individual organizations, but do not provide a complete understanding of the concerns facing the interconnected bulk power system and do not guide industry-wide efforts to develop prudent approaches to address the most material risks. NERC's roles in providing this assessment are to identify areas of concern and to make recommendations to address those concerns in a prioritized manner. This process will follow the sector framework established in the National Infrastructure Protection Plan and will be conducted with stakeholders and appropriate government agencies, including, but not limited to, DHS, DOE, FERC, and their Canadian counterparts. The assessment will serve as a foundation to guide protection goals and strategies to include the future development of Reliability Standards. The assessment will provide a complete landscape of security risks, identify significant trends and provide a common language allowing industry and government to effectively highlight both existing and emerging concerns.

IV. CONCLUSION

NERC is committed to ensuring the reliability of the bulk power system, including with respect to cyber security. NERC's actions are designed to complement those of the government, as well as actions taken by users, owners, and operators of the bulk power system. Through a better understanding of the challenges associated with

cyber security, and a commitment to a world class cyber security program, NERC seeks to enable industry to address the significant challenges to bulk power system reliability posed by cyber security threats.