

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

**BEFORE THE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
U.S. SENATE**

**Hearing on
JOINT STAFF DRAFT RELATED TO CYBERSECURITY AND CRITICAL
ELECTRICITY INFRASTRUCTURE
May 7, 2009**

INTRODUCTION

The cyber security of the bulk power system in North America remains an important concern for our nation. When I last spoke in front of a Congressional committee in September 2008, my organization, the North American Electric Reliability Corporation (NERC), had just launched a major initiative to improve its response to cyber security challenges. I am pleased to report significant progress on this front, which is a clear indication that the framework established under Section 215 of the Federal Power Act is producing results. But I remain firm in the message I communicated nine months ago: the Federal government should be given additional, carefully crafted, emergency authority to address specific, imminent cyber security threats.

My testimony today will focus on the steps NERC has taken to enhance protection of the North American bulk power system from cyber security threats, and offer NERC's views on the Joint Staff Draft, which would provide the needed federal authority.

I. ROLE OF NERC STANDARDS IN PROTECTING THE BULK POWER SYSTEM FROM CYBER ATTACK

As the international regulatory authority for the reliability of the bulk power system in North America, NERC is responsible for developing Reliability Standards applicable to all users, owners and operators of the Bulk Power System. In the United States, NERC was certified as the Electric Reliability Organization by the Federal Energy Regulatory Commission (FERC) under Section 215 of the Federal Power Act in July 2006. NERC is similarly recognized in much of Canada, with the goal of ensuring that the entire interconnected power system operates from a single platform of sound reliability practices and procedures. NERC's over 100 Reliability Standards cover long-term reliability issues ranging from vegetation management to system operator training to modeling of the bulk power system.

Eight of NERC's standards are focused on cyber security and fill a specific role in the protection of the bulk power system. The standards are comprised of roughly forty specific requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will develop the capabilities needed to secure critical infrastructure from cyber security threats. Audits of compliance with certain requirements included in the standards currently in effect, as approved by FERC on January 18, 2008 in Order No. 706, will begin on July 1, 2009.

NERC and its stakeholders recognize that the cyber security standards currently in effect can be improved and are actively working to do so in an expedited manner. As part of these efforts, NERC has worked with industry, consumer representatives and regulators to strengthen the standards both in the short-term by means of an initial six-

month revision phase, and the longer-term, through a concurrent 18-month revision phase. Phase I revisions are already complete — they were adopted by the electric industry with an 88% approval rating last week and approved by NERC’s Board of Trustees yesterday. The enhanced cyber security standards will be filed with FERC for approval promptly. We will also be filing those standards with authorities in Canada. Our work to further strengthen the cyber standards will continue, and we look forward to bringing these revisions to FERC for approval in early 2010.

One of the areas NERC and its stakeholders are working to address in the longer-term revisions was the subject of an April 7 letter from NERC Chief Security Officer Michael Assante to industry stakeholders. The letter addressed the identification of Critical Assets and associated Critical Cyber Assets that support the reliable operation of the bulk power system, as required by NERC Reliability Standard CIP-002-1.¹ In the letter, Mr. Assante called on users, owners, and operators of the bulk power system to take a fresh look at current risk-based assessment models to ensure they appropriately account for new considerations specific to cyber security, such as the need to consider misuse of a cyber asset, not simply the loss of such an asset. The letter is part of the iterative process between NERC and industry stakeholders as we work together to improve reliability. In this case, NERC gathered information about the status of implementation of the critical infrastructure protection standards and fed that information and its own insights back to the industry as part of a cycle of continuous improvement.

¹ The letter is available from the NERC website: <http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf>.

This effort demonstrates that NERC is working to address a critical element of the cyber security challenge: the educational learning curve and resulting compliance-related challenges that must be addressed to improve the cyber security of the Bulk Power System. Ensuring that each of the nearly two thousand entities that own and operate components of the bulk power system understands cyber security and the efforts needed to adequately protect the security of the bulk power system has been a priority for NERC. While efforts such as the September 23rd, 2008 cyber security summit and classified briefings for industry executives have been important components of NERC's educational efforts, the standards development process itself has contributed a great deal to raising the profile and priority of cyber security within the electric sector. Other educational efforts currently under development include a series of webinars on compliance with the critical infrastructure protection standards and further regular communication with the industry.

At the end of the day, however, preparedness efforts like those discussed above are necessary but not sufficient to protect the system against specific and imminent threats. Protecting the system from these kinds of threats is dependent in large measure on the quality and timeliness of threat analysis and risk information developed by intelligence and law enforcement professionals and, importantly, their ability to share specific, actionable information with asset owners.

II. ADDRESSING IMMINENT AND SPECIFIC CYBER SECURITY THREATS

At NERC, we are working in a number of areas to help provide or assist in the provision of the kinds of information that will help the industry better secure critical assets from advanced, well-resourced threats and other known cyber activity on an ongoing basis. Strong and proactive participation by industry volunteers thus far has been encouraging.

In these efforts, NERC collaborates with the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) on critical infrastructure and security matters on an almost daily basis. Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),² which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

NERC disseminates these findings via its voluntary alerts mechanism, which has pioneered outreach to asset owners and is virtually unmatched by other infrastructure sectors. NERC is now able to provide timely critical reliability information to security and grid operations professionals, and has demonstrated success by conducting training and using the system to send alerts, record acknowledgements and receive responses within several days. As a result, our last recommendation was met with a 94 percent response rate. The industry has been very supportive as we have worked to improve this

² 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.

process. We look forward to launching an improved secure “alerts portal” to continue to improve this system in the coming weeks.

Other efforts underway at NERC include ongoing work with industry experts to assess security risks to the bulk power system of North America. Through these assessments, NERC seeks to broaden the understanding of cyber risk concerns facing the interconnected bulk power system and guide industry-wide efforts to develop prudent approaches to address the most material risks – in both the short-term, through appropriate alerts, and longer-term, through appropriate standards. Generalized and aggregated findings generated through these assessments will be communicated with asset owners through the voluntary alerts mechanism discussed above.

We firmly believe, however, that there are circumstances where these efforts will not be adequate to identify or address specific imminent threats. NERC agrees that new, specific authority for emergency response to cyber threats is necessary. In the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government in the United States and as appropriate in Canada.

III. COMMENTS ON JOINT STAFF DRAFT

The Joint Staff Draft legislation would add a new Section 224, “Critical Electric Infrastructure,” to the Federal Power Act. The draft addresses the principal gap that NERC sees in the current law: the Federal government lacks sufficient authority to act to address an imminent and specific cyber security threat to the critical infrastructure of the United States. NERC believes that authority to act in such emergencies should be assigned to a single Federal agency. Proposed Section 224(c)(1) does this by giving the Secretary of Energy the authority to act in such circumstances. Proposed Section

224(c)(2) properly encourages the Secretary, in exercising that authority, to consult and coordinate with appropriate officials in Canada and Mexico. This encouragement is entirely appropriate, because the bulk power system in North America comprises an interconnected grid that spans two international borders.

The draft legislation goes beyond the scope of Section 215, which specifically limits standard-setting authority to apply only to users, owners, and operators of the bulk power system. The draft legislation would extend jurisdiction, for purposes of Section 224, to any entity that owns, controls, or operates systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce. At the time Congress adopted Section 215 of the Federal Power Act, providing for mandatory and enforceable reliability standards, it carefully chose the scope of jurisdiction it was granting, based on the nature of the risk and the international nature of the interconnected grid. Congress should again weigh the benefits and risks of broader jurisdiction as it considers this grant of additional authority.

Proposed Section 224(b) would give FERC authority to establish standards to address not only emergencies, but any cyber security vulnerability, defined as a weakness or flaw in the design or operation of any programmable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat. It would authorize FERC to adopt rules or orders without notice or hearing. Proposed Section 224(b) would supplant Section 215 with respect to establishing cyber security standards. The NERC standard-setting process brings together industry and security experts to develop standards that must apply to the international, interconnected grid. Developing long-term standards that apply to the more than 1800 diverse entities

that own and operate the bulk power system is a complex undertaking. Standards must apply equally to companies with thousands of employees and to those with only twenty. Additionally, the standards must not do harm. They must take into account unique component configurations and operational procedures that differ widely across the grid. Given our extensive experience in standards development, NERC firmly believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can best be found within the industry itself. Given these constraints, setting these standards should not be done without notice or opportunity to be heard, especially when the consequence of non-compliance can be significant penalties.

Sections 224(b) and 224(c) also create potentially competing emergency authorities in both the Secretary of Energy and FERC, since FERC may issue an order without notice and hearing, and there is no requirement that the Commission coordinate with the Secretary of Energy or with other potentially affected nations.

NERC believes the highest priority gap in the nation's cyber security protection is the lack of emergency authority, and proposed Section 224(c) addresses that gap.

CONCLUSION

NERC, the electric industry, and the governments of North America share a mutual goal of ensuring threats to the reliability of the bulk power system, especially cyber security threats, are clearly understood and effectively mitigated. NERC has taken a number of actions to protect the bulk power system against cyber security threats and NERC will continue its work with industry stakeholders to do so. We believe these efforts have improved and will continue to improve the reliability and security of the bulk power system. We maintain, however, that these efforts cannot be a substitute for

additional emergency authority at the federal level to address specific and imminent cyber security threats.

NERC and industry stakeholders appreciate the magnitude and priority of this issue and fully support legislative efforts to address this gap in authority as quickly as possible. Moving forward, NERC is committed to complementing Federal authority to address cyber security challenges, regardless of the form it may take. We commend this Committee for its action to date and look forward to supporting its efforts however possible.