

TESTIMONY OF MICHAEL J. ASSANTE
VICE PRESIDENT AND CHIEF SECURITY OFFICER
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BEFORE THE
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE
AND TECHNOLOGY

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

Hearing on

SECURING THE MODERN ELECTRIC GRID
FROM PHYSICAL AND CYBER ATTACKS

July 21, 2009

INTRODUCTION

My name is Michael Assante and I am the Chief Security Officer for the North American Electric Reliability Corporation (“NERC”). As the designated Electric Reliability Organization (“ERO”) in the United States and much of Canada, NERC is dedicated to ensuring the reliability of the bulk power system in North America. As part of our mission, NERC evaluates, assesses, and works with industry to address risks to the bulk power system through study, information sharing, and, where appropriate, mandatory standards. Cyber and physical security are two such risks.

The last time our organization testified before the Subcommittee, we committed to improving our response to cyber security. I am able to confidently report that we have done so. We certainly have more work to do, but NERC and the industry have made encouraging progress on this issue since May of 2008. My testimony today will provide an update on our activities, and will also provide some important perspectives for your consideration as you continue your vital work on this subject.

Notably, NERC firmly believes that additional, federal authority is needed to address specific and imminent cyber security threats to the bulk power system.

RISKS TO THE BULK POWER SYSTEM

Cyber and physical security are two of many reliability risks faced by bulk power system planners and operators.

Unlike other concerns, such as extreme weather, security-related threats can be driven by malicious actors who intentionally manipulate or disrupt normal operations as part of a premeditated design to cause damage. Cyber-related threats pose a special set of concerns in that they can arise virtually anytime, anywhere and change and emerge without warning.

While the industry deals with some physical security events, like copper theft, on a regular basis, other technical threats or hazards, such as electromagnetic pulse and space weather, are a concern and will require careful consideration to develop appropriate and effective mitigations. Cyber threats to control systems are still evolving and are not yet fully understood. The potential for an intelligent attacker to exploit a common vulnerability that impacts many assets at once, and from a distance, is one of the most concerning aspects of this challenge. This is not unique to the electric sector, but addressing it will require asset owners to apply additional, new thinking on top of sound operating and planning analysis when considering appropriate protections against these threats.

Complicating this issue, much of the information about security-related threats remains classified in the defense and intelligence communities, with restricted opportunity to share information with affected private-sector asset owners. The electric grid is placed at significant risk as a result

of limited information-sharing. NERC is not aware, however, of any cyber attacks that have directly affected the reliability of the power system in North America to date.

NERC is presently working to expand the body of analysis of physical and cyber security risks on an industry-wide basis. These efforts include analysis and consideration of specific risks and vulnerabilities as they are identified by a group of security experts from industry, security researchers, and technology vendors, dubbed “Network HYDRA”. This networked group of professionals provides important insight, feedback, and a communications vehicle to raise awareness of important security concerns.

Non-traditional risks are also the subject of a working group NERC has recently established in partnership with the Department of Energy to analyze “high impact, low probability” risks – or, more accurately, those risks whose likelihood of occurrence is uncertain relative to other threats, but that could significantly impact the system were they to occur. Officially launched on July 2, this working group will examine the potential impacts of these events on the bulk power system, focusing on influenza pandemic, space weather, terrorist attacks, and electromagnetic pulse events. The group will host an invitation-only workshop in the coming months to discuss their assessment and develop conclusions and recommendations to industry based on their work. These recommendations will be used to drive needed technology research, development, and investment and also to evaluate NERC’s current standards and initiatives, potentially driving the creation of new standards to address these issues.

In addition to these ongoing efforts, NERC is conducting a Cyber Risk Preparedness Assessment. This industry-led, voluntary assessment will focus on detection, response, and mitigation capabilities for cyber incidents. Coordinated by NERC, the assessment will look beyond NERC’s current cyber security standards for practices, procedures, and technologies that contribute to cyber preparedness across the industry. Generalized, aggregated results from the assessment will be used to inform standards development activities, alert the industry to potential areas of concern, and identify areas where research and development investment is needed. For security reasons, specific results of the assessment will remain confidential, a key condition of participation in the program.

Through these and other, more specific 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.

SCOPE OF NERC AUTHORITY

The scope of NERC’s authority as the ERO is limited to the “bulk power system,” as defined below in Section 215(a)(1) of the Federal Power Act:

- “(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.”

This authority places appropriate focus on the reliability of the bulk power system, as outages and disturbances on the bulk system have the potential for far greater impact than those on distribution systems. Elements of the power grid outside this authorization include telecommunications infrastructure and “local distribution,” which typically includes the infrastructure within urban areas and that serves many military installations.

The increasing adoption of “smart grid” and advanced metering systems on distribution systems has brought renewed focus to the appropriate definition of a bulk power system component. As grid operators rely on demand-response, rooftop solar panels, and other distribution-level assets in capacity planning and operation, the reliability of the bulk power system may become increasingly dependent on the operation of assets connected at the distribution level. While a single device would not be considered material to bulk power system reliability, in aggregate, these assets may become critical to the bulk power system.

As a result, NERC is working with the National Institute of Standards and Technology (“NIST”), the Department of Energy (“DOE”) and the Federal Energy Regulatory Commission (“FERC”) as security and interoperability standards are developed for “smart grid” technologies. Additional efforts at NERC include high-level assessment by several working groups. NERC’s technical committees are presently considering the formation of a “Smart Grid Task Force” to further evaluate these issues.

NERC MANDATORY RELIABILITY STANDARDS & COMPLIANCE

Developing mandatory standards that apply to the more than 1800 diverse entities that own and operate the North American 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.

NERC develops all its Reliability Standards through an ANSI-accredited process, which we believe provides the appropriate framework for ensuring that subject matter expertise is used to create and vet the standards. Though use of an ANSI-accredited process is not specifically required, the Federal Power Act does specify that the standards development process must “provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards....” (Sec. 215(c)(2)(D)).

In certifying NERC as the ERO, FERC found that NERC’s ANSI-accredited standards setting process meets these requirements. The standards development process is set forth in NERC’s Rules of Procedure, which FERC has approved.

The ANSI-accredited standards development process has yielded important results as NERC has revised its Critical Infrastructure Protection (“CIP”) Reliability Standards over the past year. NERC’s Board of Trustees approved revisions to eight of the nine currently-approved CIP Reliability Standards on May 6, 2009, after the standards passed industry balloting with an 88 percent approval rating. The high approval rating indicates the industry’s strong support for these development efforts, which has been vital to their success.

These revised standards were filed with FERC for regulatory approval in the United States on May 22 and are already mandatory and enforceable in parts of Canada.

NERC’s Critical Infrastructure Protection standards 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 capabilities needed to defend critical infrastructure from cyber security threats. The standards are not, however, designed to address specific, imminent threats or vulnerabilities.

Work on additional, phase-two CIP standards revisions continues, with initial industry validation on track for the fourth quarter of 2009. Modifications underway as part of the phase-two revisions include considering the extent to which elements of the Recommended Security Controls for Federal Information Systems under development by NIST can be incorporated into the CIP Reliability Standards. Also under consideration are broader foundational requirements for training and preparedness, specifically with applicability to entities who do not own or operate Critical Assets.

Additional modifications underway in this phase-two development work were the subject of a letter I sent to industry stakeholders on April 7, 2009. 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. The letter was based on initial data collections NERC has used to evaluate the implementation of the standard across the industry prior to the start of formal audits, which began for some entities on July 1, 2009. The appropriate prioritization of assets for protection is a critical component of a successful security strategy, though its implementation poses a significant challenge to industry given the complex nature of the system and the changing nature of cyber threats.

In my April 7 letter, I 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.

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

more than 1800 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.

The standards development and improvement process is producing results; however, NERC recognizes this process is not well-suited to addressing more imminent threats. As a result, NERC has been working with its stakeholders over the past year to develop and vet an alternate process for standards development to address imminent needs. This process is nearing completion and is expected to be submitted to FERC for approval before the end of the year.

ADDRESSING IMMINENT 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 DOE and the 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”), which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

NERC has in place a formal mechanism for issuing alerts to the industry about important matters that come either from NERC’s own efforts, identified vulnerabilities or attacks, or from government agencies with specific information about possible threats. Alerts issued through this mechanism are not mandatory and cannot require an entity to perform tasks recommended or advised in the alert. NERC has significantly improved this system over the past year and continues improvements through the development of a secure alerting portal, due to be complete this fall.

NERC is now able to provide timely, critical reliability information to nearly 5,000 security and grid operations professionals within minutes, and has demonstrated success by conducting training and using the system to send alerts, record acknowledgements and receive responses within several days. NERC has issued nine such alerts in 2009, with its most recent “recommendation” receiving a 94 percent response rate. The industry has been very supportive as we have worked to improve this process.

NERC’s recent work to alert the industry of the Conficker worm, including lessons learned on mitigation, involved the issuance of one recommendation, two advisories, and an awareness bulletin over the span of six months. These efforts significantly contributed to overall preparedness and awareness of the underlying vulnerability and cyber threat.

We acknowledge and believe, however, that there are circumstances where NERC’s efforts will not be adequate to identify or address specific imminent threats. Threats like those suggested by the April 8th Wall Street Journal article discussing the existence of “cyber spies” in the electric

grid, for example, have been challenging for the industry to fully evaluate and address. Without more specific information being appropriately made available to asset owners, they are unable to determine whether these concerns exist on their systems or develop appropriate mitigation strategies. A mechanism therefore is needed to validate the existence of such threats and ensure information is appropriately conveyed to and understood by asset owners and operators in order to mitigate or avert cyber vulnerabilities.

NERC and the electric industry have been working closely in confidence to evaluate threats such as those described in the article. Specific information about these efforts is bound by confidentiality agreements.

EMERGENCY FEDERAL AUTHORITY NEEDED

Preparedness and awareness efforts like the assessments, alerts, and standards discussed above are necessary, but not sufficient, to protect the system against specific and imminent threats. NERC firmly believes that additional emergency authority is needed at the federal level to address these threats, and NERC supports legislation that would give an agency or department of the Federal government necessary authority to take action in the face of specific and imminent cyber threats.

For the reasons discussed above (that reliability standards must do no harm, take unique component configurations into account, and apply equally to all bulk power system entities – including those in Canada – regardless of size or structure), 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. NERC believes an industry-based standards development process utilizing cross-border subject matter expertise will yield the best results for long-term reliability standards.

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 governmental authorities and 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 appreciates the magnitude and priority of this issue, and supports enactment of legislation 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 Subcommittee for its action to date and look forward to supporting your efforts however possible.