TESTIMONY OF DAVID N. COOK
VICE PRESIDENT AND GENERAL COUNSEL
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

Hearing on

PROTECTING THE ELECTRIC GRID: H.R. 2165, THE BULK POWER SYSTEM PROTECTION ACT OF 2009, AND H.R. 2195

October 27, 2009

INTRODUCTION

The North American Electric Reliability Corporation ("NERC") takes most seriously its role in ensuring the cyber security of the electric grid. Working with stakeholders, NERC's overall mission is to ensure the reliability of the Bulk Power System in North America. Cyber security is clearly one component of that mission. The challenges the grid faces from cyber security threats, however, are different from other reliability concerns. Unlike traditional concerns (such as vegetation management on transmission line right-of-ways) for which there is significant operating experience, digital technology changes frequently and novel potential threats can arise very quickly, requiring rapid 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 also more likely

to be driven by intentional manipulation of devices as opposed to operational events on the Bulk Power System.

All of these characteristics clearly set cyber security apart from other reliability concerns. Where 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 specific, directed action when necessary. For these reasons, NERC believes that the U.S. government needs additional emergency authority to address specific, imminent cyber security threats. With immediate emergency authority in the hands of government, NERC would be better positioned to develop and implement longer-term cyber security and critical infrastructure protection Reliability Standards.

My testimony today will focus on the process and standards in place under Section 215 of the Federal Power Act ("FPA") for ensuring that the electric grid is adequately protected against cyber and other vulnerabilities and threats. I will also offer NERC's views on elements of the pending legislation, including H.R. 2165 and H.R. 2195, to establish additional authorities to address cyber security threats to the Bulk Power System.

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 FPA in July 2006. NERC is similarly recognized in much of Canada, with the goal of ensuring that the entire interconnected North American power system operates from a single platform of sound Reliability Standards. NERC's over 100 Reliability Standards cover reliability issues ranging from vegetation management to system operator training to modeling of the Bulk Power System.

In January 2008, FERC issued Order No. 706, approving eight mandatory Reliability Standards for Critical Infrastructure Protection ("CIP Reliability Standards") developed by NERC through its ANSI-accredited standards development process.[1] These standards set forth specific requirements that are binding on users, owners and operators of the Bulk Power System to safeguard critical cyber assets.

The CIP Reliability Standards are comprised of roughly forty specific requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will help develop the capabilities needed to secure critical

[1] *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).

infrastructure from cyber security threats. Audits of compliance with certain requirements included in the standards began on July 1, 2009.

NERC recognizes, however, that while the standards in place today provide a sound starting point, they should be improved. NERC has worked with industry, consumer representatives and regulators to strengthen the CIP Reliability Standards both in the short term by means of an initial six-month revision phase, and the longer-term, through a concurrent revision phase. The initial revisions to the CIP Reliability Standards were approved by FERC as Version 2 of the CIP Reliability Standards on September 30, 2009.[2] These standards will become effective on April 1, 2010. Work to further strengthen the cyber standards is underway as phase two revisions continue.

One of the areas that must be addressed in these revisions was the subject of an April 7, 2009 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.[3] 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.

---

[2] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (2009) (Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing).

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

The letter demonstrates NERC's focus on addressing 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 approximately 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 process itself has contributed a great deal to raising the profile and priority of cyber security within the electric sector. Other educational efforts currently underway include a series of webinars on compliance with the CIP Reliability Standards and regular communication with industry.

Initial results from the most recent CIP Reliability Standards implementation survey indicate that more work is needed with industry to ensure that Critical Assets are being appropriately identified as such. For example, approximately 26 percent of generation facilities in the United States reported to NERC are presently identified by industry as Critical Assets. The specific data is a significant cause for concern regarding the current implementation of the CIP Reliability Standards for certain assets and indicates progress for others. NERC is presently engaged in further evaluating the data received and will be working with stakeholders to develop an action plan to address the issue over the coming weeks.

II. ADDRESSING IMMINENT AND SPECIFIC CYBER SECURITY THREATS

At NERC, we are working in a number of areas to 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. In its role as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[4] NERC analyzes and disseminates threat information and warnings to the electricity industry in the form of Advisories, Recommendations to Industry, and Essential Action Notifications. 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 the alerts system over the past year and continues improvements through the development of a secure alerting portal, currently in the pre-commissioning user validation phase.

Through the alerts system, NERC is 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 twelve such alerts in 2009, with its most recent "recommendation" receiving a strong 94 percent response rate.

[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 a related role in cyber and physical security issues associated with all electric facilities operated in the United States.

Preparedness and awareness efforts like the standards and alerts discussed above are necessary, but not sufficient, to protect the system against specific and imminent cyber threats. NERC firmly believes that that in the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government in the United States. 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.

III. COMMENTS ON PENDING LEGISLATION

Single Federal agency with authority to address imminent threats: Both H.R. 2165 and H.R. 2195 address 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. H.R. 2165 does this by giving FERC authority to address both certain existing cyber security threats, through interim measures to be issued within 120 days of enactment as necessary, and future emergencies involving imminent cyber security threats (proposed FPA Section 215A(b) and (c)). H.R. 2195 also assigns responsibility to FERC to establish both 1) interim measures that would supplement, replace or modify cyber security Reliability Standards that FERC finds to be inadequate to address known vulnerabilities (under proposed FPA 224B), and 2) rules or orders "necessary" to protect critical electric infrastructure against vulnerabilities or threats identified by the Department of Homeland Security, including emergency orders to protect against an

imminent threat or vulnerability issued without notice or hearing (through proposed FPA 224(c)). In contrast, S. 1462, the American Clean Energy Leadership Act, as reported by the Senate Energy Committee vests authority to act in both the Commission and the Department of Energy ("DOE"), creating potentially competing emergency authorities in both the Secretary of Energy and FERC.

Preservation of the FPA Section 215 Standards Development and Approval Process: 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 believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can be found within the industry itself. Setting long-term cyber security Reliability Standards should not be done without notice or opportunity to be heard, as valid technical feasibility concerns do exist and must be considered so that adherence to mandatory requirements in one area does not negatively impact other aspects of reliability. NERC has strong concerns regarding the tradeoffs that could be made between compliance-based decisions and those that might otherwise be in the best interests of system reliability. These concerns are also relevant for interim measures. Coordination with a

defined group of industry experts may provide an appropriate mechanism to evaluate proposed measures and identify concerns from a reliability perspective.

H.R. 2165 contains provisions to harmonize the new FERC authorities with the Reliability Standards development process. H.R. 2165 expressly provides that interim measures or actions to address existing cyber security threats are to be replaced by standards developed, approved and implemented under FPA Section 215 (proposed Section 215A(b)(2)). The legislation also specifies when interim measures are to be discontinued, including when a Reliability Standard is developed and implemented pursuant to FPA Section 215 to address the identified threat (proposed Section 215A(d)(2)). FERC orders for emergency measures or actions to protect Bulk Power System reliability against an imminent cyber security threat determined to exist by the President also are to be discontinued upon, among other things, the development and implementation of a reliability standard to address the identified threat (proposed Section 215A(e)(3)).

H.R. 2195 limits the duration of emergency orders issued by FERC without prior notice or hearing (proposed Section 224(d)), but does not otherwise provide that such rules or orders are to be replaced by Reliability Standards under FPA Section 215. Under proposed Section 224B(a)(1), interim measures to protect against known cyber vulnerabilities could replace or modify Reliability Standards established under FPA Section 215. While H.R. 2195 provides that such interim measures "may" be replaced by standards developed and approved under FPA Section 215 (proposed Section 224B(a)(2)), there is no requirement to do so.

S. 1462 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. In this way, the legislation would authorize FERC to adopt rules or orders without notice or hearing, and supplant Section 215 with respect to establishing cyber security standards in the first instance.

Coordination with Canada and Mexico: Recognizing the international nature of the North American electric grid, the legislation should assure coordination between the Federal agency with authority to address imminent cyber security threats and appropriate officials in Canada and Mexico. H.R. 2165 contains important provisions that require consultation with Canada and Mexico before the establishment of interim measures to address existing cyber security threats (proposed Section 215A(b)(1)), as well as consultation to the extent practicable before emergency orders are issued (proposed Section 215A(c)(2)). H.R 2195 contains no specific provisions in this area.
The provisions of S. 1462 dealing with the emergency authority of the Secretary of Energy encourage consultation and coordination with Canada and Mexico, but there is no corresponding requirement imposed on FERC.

Focus on the Bulk Power System: Certain aspects of the pending legislation go 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. H.R. 2195 provides that FERC rules or orders to protect against known cyber vulnerabilities or

threats may require any "owner, user or operator of critical electric infrastructure in the United States" to develop a plan to address cyber vulnerabilities identified by FERC and to submit the plan to FERC for approval (proposed Section 224B(b)). The term "critical electric infrastructure" is defined expansively as "systems and assets, whether physical or cyber used for the generation, transmission, distribution, or metering of electric energy that, in the determination of the Commission, in consultation with the Secretary of Homeland Security and other national security agencies, are so vital to the United States that the incapacity or destruction of such systems and assets, either alone or in combination with the failure of other assets, would cause significant harm to the security, national or regional economic security, or national or regional public health or safety." (Proposed Section 224(a).) The potential inclusion of distribution system assets represents an expansion of the jurisdiction under FPA Section 215, which applies to the Bulk Power System only. Similarly, S. 1462 would extend jurisdiction for purposes of cybersecurity 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. The authorities to be established under H.R. 2165 would operate consistently with the current jurisdiction under FPA Section 215.

At the time Congress adopted Section 215 of the FPA 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. 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. Congress should again weigh the benefits and risks of broader jurisdiction as it considers any grant of additional authority.

Physical vulnerabilities/threats: NERC believes addressing the present gap in authority to address specific, imminent cyber security threats is the highest legislative priority at this time. Authorities and agencies already exist to deal with risks to physical assets, including local and state police, the Federal Bureau of Investigation, and the Departments of Defense and Homeland Security.

EMP: In partnership with the DOE, NERC has recently begun an effort to assess "high impact, low frequency" 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, the effort is a culmination of high-level discussions between leadership at NERC and DOE. NERC and DOE will host a closed, invitation-only workshop on November 9-10 to examine the potential impacts of these events on the Bulk Power System. The group will focus on influenza pandemic, geomagnetic disturbances, coordinated cyber and physical attacks, and electromagnetic pulse events. Recommendations from the workshop will be used to drive needed coordination, research, development, and investment.

Treatment of sensitive information: Without more specific information being appropriately made available to asset owners, they are unable to determine whether particular cyber security 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.

All of the pending legislation contains provisions to address the need to provide information on cybersecurity threats that users, owners, and operators require to understand the nature of threats to the Bulk Power System and appropriate responses. H.R. 2165 provides for a new category of "sensitive cyber security information," which would consist of unclassified information that specifically discusses cyber security threats, vulnerabilities, mitigation plans or security procedures (proposed Section 215A(f)(1)(B)). FERC would be required to promulgate rules to provide for the release of such information to users, owners and operators in order to enable them to comply with Commission rules, orders or measures to respond to cyber threats (proposed Section 215A(f)(2)). H.R. 2195 makes the provisions of Section 214 of the Homeland Security Act of 2002, which among other things provide for procedures for the issuance of notices and warnings related to the protection of critical infrastructure and protected systems in a manner that prevents the public disclosure of critical infrastructure information, applicable to critical electric infrastructure information submitted to FERC (proposed Section 224(f)). Concerns remain over the sharing of critical infrastructure information, both at the state level and between federal entities and NERC. These issues should be addressed to ensure information is adequately protected. S. 1462 requires DOE/FERC to establish procedures to release critical infrastructure information to any entity that owns, controls, or operates critical electric infrastructure to enable them to implement rules/orders of DOE/FERC.

Such provisions may help bridge the information gap that today limits understanding of and potentially responses to cybersecurity threats and vulnerabilities.

CONCLUSION

NERC, the electric industry, and the governments of North America share a mutual goal of ensuring that threats to the reliability of the Bulk Power System, especially cyber security threats, are clearly understood and effectively mitigated. NERC believes the highest priority gap in the nation's cyber security protection is the lack of emergency authority, and all of the pending legislative proposals address this gap.

NERC appreciates the magnitude and priority of this issue and fully supports 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.