Statement of NRECA to the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Energy and Air Quality

Hearing on: Protecting the Electric Grid from Cyber-Security Threats

September 11, 2008

4301 Wilson Boulevard
Arlington VA 22203
www.nreca.coop

Executive Summary of Testimony

NRECA has worked closely with its industry counterparts, and with FERC and NERC to arrive at the legislation before you today. All parties in these discussions and negotiations recognized the seriousness of the security issues facing our nation and each worked diligently to craft legislative language that can provide swift, effective emergency protection to the bulk power system in those limited circumstances when the ERO cannot. NRECA supports the House discussion draft, with the specific language options proposed by the associations.

NRECA worked with Congress, the Federal Energy Regulatory Commission (FERC) and its industry counterparts to ensure that the 2005 Energy Policy Act (EPAct) contained strong and effective reliability provisions. NRECA has actively participated in the formation and development of the industry reliability self-regulatory organization, the North American Electric Reliability Corporation (NERC), in its role as the Electric Reliability Organization (ERO). NRECA has also been very engaged in the creation of NERC's initial reliability standards, including the cyber-security standards that FERC approved earlier this year.

For the last several years NRECA has worked closely with its electric cooperative membership on reliability issues, including those related to cyber-security. In 2005 NRECA held a series of workshops for its members on numerous cyber-security issues, including defense-in-depth practices, disaster and business continuity planning and other industry best practices for protecting cyber networks. Since June 2007 NRECA worked closely with NERC to distribute the "Aurora" mitigation measures to electric cooperatives. We also provided support to our members to help them understand the importance of these issues and the need for them to take the steps included in the mitigation measures document.

As both a participant in NERC and an interested observer of its role as the ERO, NRECA believes that the self-regulatory model is the best means of maintaining a strong, reliable bulk power system. The self-regulatory model recognizes that the electric industry overcomes some level of threat every day, ranging from those posed by inclement weather or other natural events,

to vandalism and equipment failures. The NERC structure has increased the industry's capacity to respond to a wider variety of intentional and accidental threats. Working together, FERC, NERC and industry will continue to improve an already exemplary record of maintaining and protecting the nation's electric infrastructure and continuing its high level of reliability.

For the overwhelming majority of identified threats and vulnerabilities, existing industry and NERC procedures provide the necessary response for the continued reliability of the bulk power system. There are potential improvements to ERO procedures that can increase the amount and variety of threats and vulnerabilities the industry can handle through the self-regulatory process and NERC is currently working on these issues.

However, in an age of increasing reliance on computer and web-based controls in the electric transmission and generation infrastructure, it is conceivable that some threats may be so severe and imminent that the self-regulatory model may not sufficiently protect the bulk power system. In those limited circumstances, it is appropriate to provide, in legislation, a back-stop, emergency authority which extends until the threat is mitigated, ends or is reduced to such a level that the ERO's procedures and standards can once again meet the challenge.

Introduction

Chairman Boucher, Ranking Member Upton and members of the Subcommittee, thank you for the opportunity to testify today on cyber-security issues and their potential impacts on the bulk power system.

My name is Barry Lawson, and I am the Manager, Power Delivery for the National Rural Electric Cooperative Association (NRECA). One of my primary areas of responsibility at NRECA is reliability, including those issues related to cyber-security. NRECA is a trade association consisting of nearly 1,000 cooperatives providing electricity to 41 million consumers in 47 states. As member-owned, not-for-profit organizations, cooperatives have an obligation to provide a reliable supply of electricity to all consumers in our service areas at the lowest possible price. Cooperatives serve primarily the more sparsely populated parts of our nation but cover roughly 75 percent of the nation's land mass and maintain 42 percent of the nation's electric distribution lines.

Along with many colleagues, including some of those on the panel today, I continue to work closely on reliability and cyber-security issues, with electric cooperatives, other electricity industry sectors, FERC and NERC. NRECA commends FERC, under Chairman Kelliher's leadership for its proactive outreach on the topics we are discussing today.

In January 2008, on behalf of NRECA and its members, I began a two-year chairmanship of the NERC Critical Infrastructure Protection Committee (CIPC). The CIPC is a NERC standing committee that advises the NERC Board of Trustees on issues related to critical infrastructure protection, including cyber-security. My position on the CIPC requires me to interact with NERC, Department of Energy (DOE) and Department

of Homeland Security (DHS) staff on an ongoing basis and contributes to the viewpoints I will share with you today.

Industry Cooperation in Response to the "Aurora" Vulnerability

Last fall, many members of Congress and the public at large were introduced to the concept of cyber-security when news outlets ran a story and video showing a small electric generator that was damaged during a test. The news reports said a government lab had demonstrated that computer hackers could cause physical damage to equipment through cyber means. The government labeled this vulnerability "Aurora." Today, almost no one outside the intelligence community knows what the "Aurora" vulnerability actually means from a technical or engineering standpoint. Information about the vulnerability is still classified.

The "Aurora" example and the industry's response to it highlight concepts I will discuss in my testimony today:

- NERC already has many existing procedures and reliability standards to meet ongoing threats and vulnerabilities.
- The self-regulatory structure and level of industry investment in the ERO provide the means to improve and revise existing procedures and reliability standards to address additional threats and vulnerabilities.

As a member of the NERC CIPC, I first received information about the "Aurora" vulnerability in March 2007. DHS gave CIPC members limited information about the vulnerability but strictly prohibited us from sharing that information with others even though the unclassified information provided would have been beneficial for others to receive. I could not inform key staff at NRECA or, more importantly, any of the NRECA

member cooperatives. Several months later DHS then placed limited information into a document that NERC relied on to distribute as mitigation measures to the industry on June 21, 2007. It was at that time I was first permitted to share the information with key staff at NRECA and NRECA member cooperatives. Although the mitigation measures did not reveal the specific technical or cyber vulnerability the actions would protect against, cooperatives, and other utilities that own or operate bulk power system facilities, used their collective expertise to implement the measures on their individual systems to mitigate the Aurora vulnerability.

NERC Currently Equipped to Handle Many Threats and Vulnerabilities

The Subcommittee should be aware of the procedures and standards used to respond to "Aurora." These existing NERC processes allow NERC and the industry to assess a wide variety of threats and vulnerabilities and then devise and implement effective industry responses.

Under the existing rules and procedures created by NERC and approved by FERC, NERC has the capability to deal with a wide range of cyber threats. For issues that can be addressed with longer-term solutions, NERC and industry develop standards as prescribed by FERC under Section 215 of the Federal Power Act as passed in Section 1221 of EPAct. NERC's standards development process is designed to develop mandatory reliability standards for users, owners and operators of the bulk power system. This process can sometimes be lengthy to accommodate the highly technical nature of the subject matter, but it can also be shortened if conditions require expediency. NERC's normal process can take a number of months to longer than a year to develop a standard. However, NERC also has in its Reliability Standards Development Procedure, as

approved by FERC, two special procedures for developing standards more quickly. The Urgent Action process was developed to approve standards within a few months and the Emergency Action process was developed to approve standards within a few weeks if necessary. The Urgent and Emergency Action processes should be used to the extent they are needed for the expedient development of reliability standards, including those related to cyber security.

In addition, NERC has in its Rules of Procedure, as approved by FERC, the ability to distribute advisories on topics that are important for industry to address. There are three levels of advisories, including the most critical advisory level entitled "Essential Action." We strongly support NERC's use of the advisory tool to quickly – within hours or days – distribute important information to the industry for action.

Improvements to Existing NERC Procedures Can Help Meet Additional Threats and Vulnerabilities

On July 7, 2008, NERC wrote its Board of Trustees and industry stakeholders to explain the changes and improvements it plans to make regarding its focus on cyber-security. These ongoing NERC efforts to improve its ability to respond quickly and efficiently to cyber-security threats and vulnerabilities are critically important to reliability of the bulk power system.

I want to highlight for you three specific efforts by NERC. First, NERC has recently hired a Chief Security Officer (CSO), who will be responsible for coordinating cyber-security matters across all NERC activities. We look forward to working closely with the new CSO. Second, we support NERC's plan to develop an Emergency/Crisis

standards setting process for cyber-security. Finally, we agree with NERC that there is a need to develop closer coordination with government on cyber-security issues.

Substantial and Imminent Threats May Require Exercise of Emergency Authority

NRECA, working closely with its counterparts across the electric industry, agrees there is potential for some threats and vulnerabilities so imminent and substantial that even revised and strengthened NERC procedures cannot assure the timely distribution of information and direction to industry to effectuate an adequate industry response to protect the bulk power system.

In those limited circumstances, when the President of the United States has determined that emergency action is warranted, FERC should have the authority to issue orders, after consultation with the industry and relevant governmental authorities in Canada and Mexico, that directly address the vulnerability and/or threat and the necessary mitigation actions needed to protect the bulk power system.

Answers to Specific Subcommittee Questions

In requesting my testimony, you asked me to address several specific points about the nature and urgency of the threat to the electric system from cyber-security breaches. NRECA is in agreement with the points in the Edison Electric Institute's (EEI) testimony regarding operational issues. My answers are based on my own experience as a member of the CIPC and a resource for operational and cyber experts working on-the-ground at cooperatives.

(a) The degree and urgency of the perceived risks to the bulk power system and those it serves and (b) the evidence that such risks are real based on experience (limited to unclassified information).

The electric industry has decades of experience in assessing a wide variety of threats to critical infrastructure assets. Electric utilities have focused on cyber threats increasingly over time, in proportion to the increasing use of automated components in generation and transmission of electricity.

It is important to note that each utility has a mix of older and newer equipment. Many parts of the bulk power system operating today still rely on mechanical components that are not programmable and these older assets in many cases are not vulnerable to cyber threats as is some of the newer equipment.

Since 2001, I have been involved in critical infrastructure protection issues, including those related to cyber. I can tell you based on my own experience that the cooperative industry takes cyber threats and vulnerabilities very seriously. However, to my knowledge, including that gained serving on the CIPC for six years, there are no documented cases of successful attempts to damage the North American bulk power system through cyber channels.

(c) The extent to which the utility industry and other key participants in grid operations are or are not already prepared or currently undertaking protective measures.

My job at NRECA requires me to assist electric cooperatives that own or operate bulk power system assets in complying with FERC's mandatory reliability standards. Based on workshops, presentations and in regular interactions with our membership, I believe cooperatives are addressing known cyber threats and vulnerabilities.

(d) The scope of damages that could be inflicted if adequate protective measures are not taken and (e) the costs and time required for mitigation of such risks.

The scope of potential damages is as wide as the scope of potential events. If utilities receive more timely and detailed information from intelligence sources about threats and vulnerabilities and their engineering, cyber and mechanical implications, utilities can then better assess the mitigation steps needed and balance those with the potential likelihood of a successful attack. Utilities must also consider the reliability impacts of any action concerning their generation and transmission assets, including those posed by mitigation measures.

(f) How protection from cyber-security breaches can be assured even as the electricity industry continues to evolve toward "smart grid" capabilities including greater use of digital information and controls.

Like our industry counterparts, cooperatives are moving steadily toward smart grid applications where value to consumers is clearly demonstrated. In fact, a 2006 FERC study found that cooperatives lead the industry in installation of smart meters, and for years have directly managed over six percent of cooperative peak load. Cyber-security, especially for systems involving higher amounts of cyber components is very important. The industry, local, state and federal governments, and the vendor community must work closely together to mitigate vulnerabilities and excess costs that can arise when government policies, industry practices and technological goals do not match.

I was also asked to address several specific points about the Committee's draft cyber-security legislation. NRECA agrees with our industry counterparts about the specifics of the legislation and supports the written testimony provided by American Public Power Association and EEI on these points.

Conclusion

In conclusion, NRECA supports the House discussion draft, with the specific language options proposed by the associations. Like our industry counterparts, NRECA is prepared to assist the Subcommittee and full Committee with advancing this legislation. NRECA also looks forward to the continued cooperation with FERC that has been a hallmark of the process of arriving at this draft. I look forward to answering any questions you may have.