Statement of the North Carolina Electric Membership Corporation

to the United States House of Representatives

Committee on Small Business, Subcommittee on Healthcare and Technology

Hearing on Cybersecurity

December 1, 2011

Executive Summary

Electric cooperatives (co-ops) 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 aimed at protecting the Bulk Power System (BPS), also called "the grid." Co-ops actively participated in the formation and development of the industry reliability self-regulatory organization, the North American Electric Reliability Corporation (NERC). Six years later, co-ops are deeply engaged in the development of NERC's reliability standards, including the cybersecurity standards.

North Carolina Electric Membership Corporation (NCEMC) is a "registered entity" on the NERC Compliance Registry because of the size and function of some of its transmission and generation assets. It also handles NERC compliance for some of the distribution cooperatives which collectively own NCEMC. NCEMC has first-hand experience with the responsibilities and burdens related to creating and implementing a functional set of reliability and cybersecurity standards.

Like all cooperatives, NCEMC takes its responsibility to protect the grid very seriously. NCEMC recognizes that reliable electric service and national security are both of paramount importance. Multiple discussions are taking place in Congress and within the Administration about how to increase cybersecurity protections for critical infrastructure. NCEMC and NRECA commend the work of Speaker John Boehner's Cybersecurity Task Force and the leadership of Rep. Mac Thornberry.

NCEMC and its national trade association, the National Rural Electric Cooperative Association (NRECA), believe the NERC process is working well. The process could be

strengthened by narrowly targeted legislation that 1) provides the federal government the ability to react quickly to severe, imminent cyber threats and 2) increases the amount of timely, actionable information flowing to grid owners and operators. The scope of any proposed legislation should be limited to those assets and systems which are realistic targets of a cyber threat and which could have significant impact on the security of the BPS. Casting too wide a net could bring entities like distribution co-ops and other small businesses under potentially very burdensome regulatory requirements with little or no benefit to grid security.

Introduction

Chairman Ellmers and Ranking Member Richmond, and all members of the Subcommittee, thank you for the opportunity to testify today on electric cooperatives' responsibilities to provide cybersecurity protections to one of the nation's most critical infrastructures, the bulk power system, also known as "the grid." My name is David Beam and I am Senior Vice-President, Corporate Strategy, at NCEMC. As the corporate compliance officer for NCEMC, I have oversight responsibilities in the areas of energy risk management and regulatory compliance. In this capacity, I am the senior manager responsible for NERC reliability compliance and cyber security. I bring over 30 years experience in the electric utility industry to these roles.

While my testimony and remarks today are made on behalf of NCEMC, I would also like to briefly mention the National Rural Electric Cooperative Association. NRECA is a trade association consisting of over 900 cooperatives providing electricity to 42 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. All but five of the nation's distribution electric cooperatives are considered small businesses under guidelines set by the Small Business Administration[1]. All of the distribution cooperatives that own NCEMC are small businesses.

In my testimony today I hope to achieve the following:

1. Provide a basic explanation of the Bulk Power System and how it differs from and is isolated from the distribution system.

2. Offer some background on the Energy Policy Act of 2005 and the purposes of NERC to help explain the origins of the cybersecurity regime NCEMC complies with today.

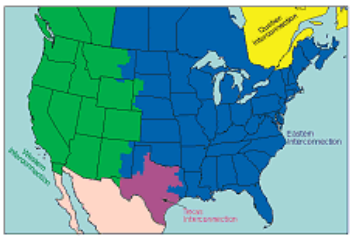
3. Share information about how NCEMC works to achieve a culture of compliance with the NERC standards and industry cybersecurity best practices.

4. Contribute NCEMC's and NRECA's general views on the state of cybersecurity legislation and the potential impact of new legislation.

The Bulk Power System and the Distribution System

The U.S. has three major bulk power systems or grids: (a) the Eastern Interconnect**,** consisting of the eastern two-thirds of the United States; (b) the Western Interconnect**,** consisting primarily of the Southwest and areas west of the Rocky Mountains; and (c) ERCOT, consisting mainly of Texas. NCEMC resides in the Eastern Interconnect.

[1] Annual retail sales of less than four million megawatt hours of electricity.



(Map obtained from the Energy Information Administration)

Generally speaking, NERC standards apply to the BPS, which NERC standards refer to as the "bulk electric system." NERC's general definition of the bulk electric system is "as defined by the regional reliability organization[2], the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition. A bulk power system consists of high-voltage connections between individual utilities designed to permit the transfer of electrical energy from one part of the network to another." NERC, its regional entities and an industry standards drafting team are currently engaged in a process to revise the BES definition.

Contrary to popular belief, a remote hacker cannot easily access the telecommunications systems that overlay parts of the bulk power system. Utilities employ multiple layers of defenses and ensure that the telecommunications systems used to operate the generation and transmission assets are separate and distinct from the telecommunications systems that are visible to the public. The types of defenses employed by NCEMC are described in more detail in the "NCEMC Cybersecurity Operations" section of this testimony.

The electric industry has deep experience with assessing and mitigating a wide variety of threats to critical infrastructure assets. For example, we've restored power after hurricanes and ice storms for decades. Electric utilities have focused on cyber threats increasingly over time, in

[2] NCEMC is part of the Southeastern Reliability Corporation (SERC).

proportion to the increasing use of automated components in generation, transmission and distribution 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; in many cases these older assets are not vulnerable to cyber threats.

Distribution utilities receive power from the bulk power system and transmit it to retail customers. Because outages at the distribution level cannot cascade back up to the bulk power system, NERC standards do not generally cover distribution lines and substations. However, with the advent of the smart grid and increasing installations of smart meters across distribution systems, electric cooperative member-consumers are asking questions about the cybersecurity of telecommunications-enabled components in smart meters and appliances. In acknowledgement of the consumer interest in security protections for their utility usage data and communications with their electric service provider, NRECA, through its Cooperative Research Network (CRN), has developed a "Guide to Developing a Cyber Security and Risk Mitigation Plan." Using these tools cooperatives (and other utilities) can start immediately to strengthen their security posture and chart a path of continuous improvement. The plan includes:

1. **Cyber Security Risk Mitigation Checklist.** A list of activities/security controls necessary to implement a cyber security plan, with rationales.
2. **Security Questions for Smart Grid Vendors.** CRN is encouraging co-ops to include these questions in their RFPs for smart grid components. The questions are designed to facilitate a frank and open dialogue on cyber security with those who make and sell components.

3. **Interoperability and Cyber Security Plan.** The Interoperability and Cyber Security Plan (ICSP) examines risk management, identification of critical cyber assets, and electronic security perimeters, among other issues.

Existing NERC Procedures Guide Industry through Threats and Vulnerabilities

In order to increase the protection afforded to the bulk power systems or grids, throughout the country, Congress approved a mandatory and enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005. It is commonly referred to as "Section 215" because it resides in Section 215 of the Federal Power Act. Under Section 215, NERC employs a stakeholder-driven process involving electric power industry experts, regional entities, Federal Energy Regulatory Commission (FERC) staff and other government representatives, to draft mandatory and enforceable reliability and cyber security standards that apply across the North American grid.

When it comes to reliability issues, the investor-owned, municipal, cooperatively-owned and merchant sectors of the electric power industry work closely together in many forums. Regardless of ownership structure, utilities dedicate thousands of employee hours to the standards development process and routinely share information through NERC and other discussion forums. I am personally involved in standards development and policy through my role as a member of the SERC Board Executive Committee. NCEMC staff work with other utilities through SERC committees, NRECA and other forums to review and provide input into industry standards.

Section 215 has a stakeholder-driven process because electric utility owners and operators are experienced and knowledgeable about how to provide reliable electric service at a

reasonable cost to our customers, and we understand how our complex systems are designed and operated. We are uniquely positioned to understand the consequences of a potential malicious act and the proposed mitigating actions needed to prevent such exploitation, including ensuring against unintended consequences of remedial actions.

FERC has the authority to approve or remand standards that emerge from the stakeholder process. NERC and FERC can levy fines on utilities that violate the standards and have done so. Additionally, FERC can direct NERC to develop new or revised reliability standards within a specific timeframe. The reliability standards cover physical and cyber aspects of the grid. 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.

NERC also has authority to distribute alerts on topics that are important for industry to address. There are three levels of alerts: Advisory, Recommended Action and - the most critical advisory level - Essential Action. Recommended Action and Essential Action Alerts have mandatory reporting requirements that typically demonstrate what action an entity has taken. NERC and the industry have used the alert process successfully to distribute critical information related to many issues, including Aurora, Stuxnet, Night Dragon, geomagnetic disturbances and many other cyber and operational issues.

NCEMC Asset Overview

NCEMC is a generation and transmission cooperative that provides wholesale power and other related services to 25 of the 26 electric cooperatives incorporated in the state of North Carolina. For 20 of the cooperatives, called Participating Members (PMs), NCEMC is the full

requirements power supplier. For 5 of the cooperatives, called Independent Members (IMs), NCEMC provides partial requirements capacity and energy entitlements from designated resources, pursuant to a Wholesale Power Supply Agreement. The twenty-sixth cooperative, French Broad EMC, is not a member of NCEMC.

The service territories of NCEMC's member distribution EMCs are located within the balancing areas of Progress Energy Carolinas ("PEC"), Duke Energy Carolinas ("Duke Energy"), and PJM Interconnection LLC[3] ("PJM"). Therefore, NCEMC's system consists of three distinct areas, identified as supply areas, located entirely in the state of North Carolina.

NCEMC is registered as the responsible entity for reliability and cyber-security compliance for its own assets as well as those of its Participating Members. These assets include generation and transmission facilities and associated protection equipment and procedures.

NCEMC relies on the transmission systems of Duke Energy, Progress Energy and PJM to transfer the power it generates and purchases to the 198 delivery points of the PMs; 125 in Progress, 46 in Dominion, and 27 in Duke. 151 of those are Transmission delivery points and 47 are Distribution. NCEMC's all-time peak load was 3232 MWs at generation in December, 2010. NCEMC and its members own roughly 17 miles of 230kV transmission lines along with a large amount of 115kV transmission. All of these facilities are radial, load-serving transmission with one source. In addition, NCEMC's members operate extensive distribution systems which deliver power to retail consumers, but are not part of the BES.

Since 1980, NCEMC has been a part owner in the baseload Catawba Nuclear Station located in York County, South Carolina. Duke Energy operates and maintains the station, which has been operational since 1985. NCEMC's ownership share consists of 61.51 percent of Unit 1,

[3] The PJM Interconnection is a regional transmission organization (RTO) that coordinates the movement of wholesale power in 13 states, including North Carolina. It operates a competitive wholesale market and manages the high-voltage electricity grid.

approximately 704 MW (1,145-MW unit capacity) and 30.754 percent in the common support facilities of the station. NCEMC's ownership entitlement is guaranteed through a reliability exchange between the Catawba Nuclear Station and the McGuire Nuclear Station located in Mecklenburg County, North Carolina. The reliability exchange results in an effective guaranteed capacity of 681.9 MW.

NCEMC owns and operates 622 MW of aero-derivative combustion turbines on a site in Anson County and a site in Richmond County, both in North Carolina. These peaking resources operate on natural gas as primary fuel, with diesel storage on-site as a secondary fuel. These units have been in commercial operation since 2007.

NCEMC also owns and operates two internal-combustion, diesel-powered generating stations on the Outer Banks of North Carolina (located on Ocracoke Island and in Buxton). These super peak units, which began commercial operation in 1991, have a combined capacity of 18 MW and are used primarily for peak shaving and voltage support.

NCEMC Cybersecurity Operations

Compliance Organizational Overview

NCEMC follows exacting procedures to ensure compliance with NERC standards. The NCEMC Board of Directors has approved a compliance policy that affirms NCEMC's on-going commitment to oversee compliance with applicable state and federal laws and regulations and authorizes the establishment of a formal compliance program. The comprehensive Compliance Program is intended to foster awareness and commitment to compliance by all employees, provide for effective preventative measures to discourage non-compliance, facilitate prompt detection, cessation and reporting of violations, and establish effective remediation measures should violations occur.

NCEMC has devoted significant financial and human resources to assuring reliability and cybersecurity. As mentioned above, I serve as the NCEMC Compliance Officer, overseeing all our reliability and cybersecurity compliance activities. In addition, I serve on the SERC Board of Directors and Board Executive Committee, where I am in a position to monitor and provide input to the compliance enforcement process. NCEMC has employed a full time compliance coordinator, whose sole responsibility is to manage compliance with reliability and cybersecurity standards. In addition, NCEMC employs a compliance team of subject matter experts (SMEs) who have individual responsibility for compliance with their assigned cybersecurity and reliability standards. The SMEs are also engaged in the standards process through participation on various SERC committees, the NERC standards process and through NRECA. . NCEMC also utilizes the services of outside contractors to audit and provide recommendations for improving our reliability and cybersecurity compliance. Additionally, there is at least one employee at each of NCEMC's Members who is assigned responsibility for compliance with reliability and cybersecurity standards.

The Compliance Program lays out a general structure for managing compliance with all corporate compliance obligations. Oversight for each compliance function is assigned to a Compliance Manager. A separate, written Compliance Plan is established for each compliance function laying out specific processes and procedures for ensuring compliance consistent with principles outlined in the Compliance Program.

The Compliance Plan lays out the structure, processes and procedures for managing compliance with all applicable reliability and cybersecurity standards. The Compliance Plan was developed by the Compliance Manager and the Compliance Team, with oversight from the

Compliance Officer. The final Compliance Plan was reviewed by senior management and approved by the Compliance Officer.

The NERC Compliance Plan undergoes an annual program review conducted by the Compliance Manager, the Compliance Team and the SMEs. As part of this process, the plan is reviewed for any opportunities for improvement and the Compliance Manager recommends any changes or additions. Any recommended changes are reviewed and approved by the Compliance Officer.

Cyber Security Technology Overview

NCEMC has made significant technology investments in order to assure compliance with NERC cybersecurity standards. Some are just common sense and would be best practices even without the standards. For example, users are required to change password every 90 days and our data center is secured via the electronic badge access. Access to our data center is logged.

Other measures are more involved and costly. For example, NCEMC operates two autonomous networks - a secure network for business systems and a secure network for Energy Management Systems (EMS). No internet traffic (email, word processing etc.) is allowed on the EMS network. Remote access into the EMS network is monitored and controlled through Virtual Private Network. Each access granted has to be requested and authorized before use and terminated as soon as the job is complete. All the remote access is logged and monitored.

Looking even more closely at NCEMC's efforts, Security Event Incident Management (SEIM) systems are used to proactively monitor networks "24x7x365" for anomalies and unauthorized access. Firewalls are used at the internal and external network access points.

Substation communications are used to collect telemetry data but no command and control is available for the substations.

Finally, to document adequately that NCEMC has complied with all the substantive NERC requirements, NCEMC employees spend a great deal of time performing regular testing of the systems and processes described above. We conduct an annual disaster recovery test to ensure our ability to promptly recover all critical systems in the event of a major event. We also perform rigorous audits internally and pay external firms for regular audits. SERC may audit our compliance at any time.

Viewpoints on Future Cybersecurity Legislative Proposals

Since cybersecurity threats are constantly evolving, the electric cooperative sector recognizes the potential for some threats so imminent and severe that even the comprehensive, carefully designed NERC procedures and standards cannot assure the timely distribution of information and direction to industry to achieve an adequate industry response to protect the bulk electric system. In those limited circumstances, when the President of the United States has determined that emergency action is warranted, the federal government should have the authority to issue orders that directly address the threat and the necessary mitigation actions needed to protect the bulk power system. Electric cooperatives, along with the entire electric power industry, have supported this additional limited authority for over three years.

However, any future legislation seeking to create new authorities that largely duplicate existing FERC authority under Section 215 of the Federal Power Act could substantially undermine the existing reliability standards regime. This is most likely to occur if legislation

emerges seeking to provide additional FERC authority to write standards or issue orders concerning grid vulnerabilities[4], as opposed to imminent threats.

When addressing cybersecurity, we encourage Congress to focus its attention on the immediate, narrow issues at hand: 1) the need for the federal government to issue emergency orders very quickly if the bulk power system is under an imminent threat of cyber attack; and 2) the need for the electric power industry to hold more security clearances in order to better facilitate the sharing of timely, actionable information needed to fashion responses to such threats. The scope of any proposed legislation should be limited to those assets and systems which are realistic targets of a cyber threat and which could have significant impact on the security of the BPS. Casting too wide a net would bring entities like distribution co-ops and other small businesses under potentially very burdensome regulatory requirements with little or no benefit to grid security.

NCEMC and NRECA agree with and appreciate the observations and recommendations issued in Speaker Boehner's Cybersecurity Task Force Report (Oct. 2011), including:

- *"Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity at these facilities using existing regulators." (p. 9)*
- *"Industries with identified critical infrastructures should have full and complete participation in the development of cybersecurity standards and best practices. (p. 9)*
- *"The Department of Homeland Security should work with other regulators to help coordinate security standards across sectors … ." (p. 9)*
- *"… [G]reater sharing of information is needed within industries, among industries and between government and industry in order to improve cybersecurity and to prevent and respond to rapidly changing threats."(p. 10)*

[4] Vulnerabilities are potential weaknesses which could be exploited to attack the grid. However, vulnerabilities typically have longer lead times and do not pose an immediate threat. The NERC-FERC regime as it exists today has guided the electric sector through multiple vulnerabilities, as noted above in my testimony.

Conclusion

Thank you for the opportunity to testify at today's important hearing. I appreciate the opportunity to discuss cybersecurity issues with the members of the House Small Business Subcommittee on Health and Technology. NCEMC and NRECA are ready, willing and able to serve as a resource on this issue which has the potential to impact our grid, economy and national security.