Statement of the National Rural Electric Cooperative Association
to the United States House of Representatives

Committee on Energy and Commerce

Energy and Power Subcommittee

"Protecting the Electric Grid: The Grid Reliability and Infrastructure Defense Act."

May 31, 2011

4301 Wilson Boulevard
Arlington VA 22203
www.nreca.coop

Executive Summary

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 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 and its members have also been very engaged in the development of NERC's reliability standards, including the cybersecurity standards.

The self-regulatory model recognizes the expertise that resides throughout the electric power industry and is the best means of maintaining a strong, reliable bulk power system. Each day, the electric power industry overcomes some level of threat, ranging from those posed by inclement weather or other natural events, to vandalism, equipment failures and cyber events. The NERC reliability standards support industry's capacity to respond to a wide variety of intentional events and natural disasters.

For the overwhelming majority of identified threats, existing industry and NERC procedures, standards and alerts support the necessary response from industry for the continued reliability of the bulk power system. However, with increasing reliance on computerized and telecommunications-enabled controls in electricity infrastructure, some threats may be so severe and imminent that the self-regulatory model - without the benefit of classified intelligence - may not be able to respond as quickly as needed to sufficiently protect the bulk power system. In those limited circumstances, it is appropriate to provide a back-stop, federal emergency authority which extends until the

threat is mitigated, ends or until NERC can adequately address the threat through standards and/or alerts.

Existing industry and NERC procedures, standards and alerts support the necessary response from industry for vulnerabilities. These capabilities and the private-public partnership will be improved as the federal government provides more timely and actionable information and intelligence to the electric power industry.

Introduction

Chairman Whitfield, Ranking Member Rush and members of the Subcommittee, thank you for the opportunity to testify today on cyber-security threats and vulnerabilities, their potential impacts on the bulk power system, and the draft legislation known as the "GRID Act."

My name is Barry Lawson, and I am the Associate Director, Power Delivery and Reliability 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 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.

While my testimony today is offered on behalf of electric cooperatives, I want to also recognize the long-standing partnership among all sectors of the electric power

industry when it comes to reliability and cybersecurity. NRECA is part of an industry wide coalition which includes several major trade associations representing the full scope of electric generation, transmission and distribution in the United States, as well as state regulators, Canadian interests and large industrial consumers. Participating in the coalition are: the American Public Power Association, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association, the Transmission Access Policy Study Group, and the Utilities Telecom Council. Rarely do all of these groups find consensus on public policy issues, but among us, there is unanimous support for ensuring that the public and private sectors can continue to work together effectively to maintain and improve cyber and grid security. My testimony focuses on the value of this cooperative relationship, the unique nature of threats and vulnerabilities facing to the power grid, and the ongoing efforts of the nation's electric sector to respond to threats and vulnerabilities.

Along with many colleagues, including some on the panel today, I work on reliability and cyber and grid security issues with electric cooperatives, other electricity industry sectors, FERC and NERC. From 2008 to the end of 2011, on behalf of NRECA and its members, I chair 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 at NRECA and my role on the CIPC requires me to interact with NERC, the Department of Energy (DOE) and the Department of Homeland Security (DHS) on an ongoing basis

and contributes to the viewpoints I will share with you today. In addition, I am an active member of the Electric Sector Coordinating Council – the ESCC -- which interacts with our sector specific agency – DOE – and other federal government agencies and critical infrastructures on the policy level issues related to critical infrastructure protection. Mr. Cauley from NERC is the Chair of the ESCC. For the last decade, I have been involved in critical infrastructure protection issues, including those related to cyber security. I can tell you based on my own experience that the electric power industry takes cyber threats and vulnerabilities very seriously. However, to my knowledge, including that gained serving in various leadership roles, there are no documented cases of successful attempts to damage the North American bulk power system through cyber channels.

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, 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 and these older assets in many cases are not vulnerable to cyber threats.

Existing NERC Procedures Guide Industry through Threats and Vulnerabilities

Congress approved a mandatory and enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005, known as Section 215. Under Section 215 NERC works closely with electric power industry experts, regional entities, FERC staff and other government representatives, to draft mandatory and enforceable

reliability and cyber security standards that apply across the North American grid, including Canada and parts of Mexico. Electrons don't recognize borders.

FERC has the authority to then approve or remand those standards as they apply in the United States. The Canadian provinces have voluntarily entered into MOUs with NERC to determine how they will address compliance with the approved standards. NERC and FERC can levy fines on U.S. entities 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. Therefore, NERC today 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.

The standards process can sometimes be lengthy to accommodate the highly technical nature of the subject matter, but it can also be shortened when needed. The NERC Standards Process Manual, as approved by FERC, provides for an expedited standards development process that can significantly shorten the standards development timeline. Additionally, NERC also has a process for developing standards in a confidential manner, in response to and in consideration of, national security and emergency issues.

The NERC Rules of Procedure also provide NERC with the authority to distribute alerts on topics that are important for industry to address. FERC reviews these alerts but they are distributed by NERC. 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. We strongly support NERC's use of the alert tools to quickly – within hours or days – distribute important information to the industry for action. In fact, NERC and the industry have used the alert process successfully to distribute critical information related to many issues, including Stuxnet, Night Dragon, geomagnetic disturbances and many other cyber and operational issues. NERC is required to provide reports to FERC on Recommended and Essential Action alerts explaining the level of action industry has taken. To date, those reports have shown that industry takes these alerts seriously by demonstrating the high level of industry response to the issues identified in the alerts.

Viewpoints on "GRID Act" Discussion Draft

NRECA, working closely with its counterparts across the electric industry, agrees there is 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 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, the federal government should have the authority to issue orders (after coordination with the industry and relevant governmental authorities in Canada and Mexico) that directly address the threat and the necessary mitigation actions needed to protect the bulk power system.

Our over-arching concern is that the draft GRID Act creates new authority for FERC concerning vulnerabilities that largely duplicates existing FERC authority under

Section 215 of the Federal Power Act and could substantially undermine the existing reliability standards regime. We question whether FERC has the technical or intelligence-handling expertise to exercise such a broad new authority. Operationally, this new authority could result in the establishment of potentially conflicting or different cybersecurity standards in the U.S. and Canada. We urge the Subcommittee 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 receive timely, actionable information to facilitate responses to such threats.

GRID Act Section 2(b): Emergency Response Measures

The draft gives FERC new authorities to issue emergency orders if the President notifies the Commission that an "imminent grid security threat" exists. When the federal government has actionable intelligence about an imminent cyber threat to the electric grid, there won't always be time for classified industry briefings or thorough development of mitigation measures. In these limited circumstances, the federal government should have the authority to direct the electric power industry on the needed emergency actions until the threat ends, is mitigated or a one-year period has elapsed.

GRID Act Section 2(c): Measures to Address Grid Security Vulnerabilities

The draft gives FERC the authority, if it determines there is a grid security vulnerability that existing NERC reliability standards do not address, to issue a rule or order requiring any owner, operator or user of the U.S. bulk-power system to implement measures to protect against the vulnerability. The draft encourages FERC to consider recommendations from NERC. The draft also lists three specific vulnerabilities FERC

must address with this new authority[1]. This section and the new authority it seeks to provide to FERC are very concerning to our industry. This subsection represents a fundamental alteration of the Section 215 reliability regime that could result in duplicative, conflicting, or unworkable reliability standards across the diverse North American grid.

Furthermore, FERC already has the authority to instruct NERC to develop or modify a standard on any topic, including but not limited to, the three vulnerabilities listed in the draft GRID Act. Section 215(d)(5) reads:

> "The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."

Vulnerabilities are potential events with longer lead times and without the accompanying intelligence that the vulnerability will be exploited with impact. Vulnerabilities present a lower urgency and risk level than threats and the debate over how to address them should recognize that vulnerabilities alone do not adversely impact the reliability of the electric grid. Infrastructure users, owners and operators take vulnerabilities very seriously and should act appropriately to address vulnerabilities before any are potentially exploited. Electric infrastructure owners and operators have

[1] At subsection 2(c)(2), the draft instructs FERC to issue a rule or order to any user, owner or operator of the U.S. bulk power system requiring the implementation of measures to protect the bulk-power system against a vulnerability known as "Aurora." Subsection 2(c)(4) instructs the Commission to issue an order to NERC to produce a standard on geomagnetic storms. Subsection 2(c)(5) instructs the Commission to issue an order directing NERC to produce a standard on the availability of large transformers.

every incentive - ranging from financial considerations to the fundamental obligation to serve our customers with reliable, safe and affordable power - to take the necessary steps to protect the grid from threats and vulnerabilities.

If intelligence agencies or FERC have identified grid vulnerabilities or threats, industry needs to be made aware of them immediately so necessary actions can be taken. The electric industry wants a safe, secure and reliable grid and we need access to timely and actionable federal government intelligence to help us to do that job to the best of our abilities.

GRID Act Section 2(g)(3): Security Clearances and Communication

Our sector can be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats and vulnerabilities because of limitations on its access to classified information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. The government is able to detect threats, evaluate the likelihood or risk of a malicious attack, and utilize its expertise in law enforcement. Industry participants accountable for protecting critical infrastructure can respond to threats and address vulnerabilities even more effectively with timely, clear and actionable information from government partners.

On the other hand, the electric industry is experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operated. The electric industry is 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. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more reliable and secure electric grid for the benefit of our customers.

In order for the electric power sector to partner effectively with government to protect the grid when vulnerabilities or threats arise, we need timely, actionable information and intelligence from government. Additional selected experts in the electric industry need to have higher levels of security clearances so that trusted people within our sector with industry knowledge can assist the federal government in fashioning a response to threats and vulnerabilities and help direct needed industry actions.

The draft legislation seeks to improve information sharing between the federal government and the electric power industry, with provisions aimed at expediting the acquisition of crucial security clearances to key personnel and requiring the distribution of timely and actionable information regarding threats and vulnerabilities. We appreciate the Subcommittee's support on this critical aspect of grid protection.

Conclusion

Thank you for the opportunity to testify at today's important hearing. The electric industry looks forward to working with the Subcommittee and full Committee to fashion legislation that will maintain the industry-government partnerships that are already making the grid more secure and supply the additional narrow authority that is needed if a severe and imminent cyber threat emerges.