




**National Rural Electric  
Cooperative Association**

A Touchstone Energy® Cooperative 

Glenn English  
Chief Executive Officer

February 15, 2013

The Honorable Edward J. Markey  
Ranking Member  
House Natural Resources Committee  
2108 Rayburn House Office Building  
Washington, DC 20515

The Honorable Henry A. Waxman  
Ranking Member  
House Energy & Commerce Committee  
2204 Rayburn House Office Building  
Washington, DC 20515

Dear Ranking Members Markey and Waxman:

The National Rural Electric Cooperative Association (NRECA) and its members take very seriously the importance of vigilance against cybersecurity risks and the issues highlighted in your broadly-circulated letter of January 17, 2013. While our members, who serve nearly 42 million consumers in 47 states (excluding Massachusetts, Rhode Island and Connecticut), are on the front lines, NRECA supports them by working with policymakers and stakeholders to strengthen the public-private partnerships that are an essential component of grid protection.

It is precisely because of our commitment to responsible grid protection that we and our members are concerned that your letter asks for sensitive information and in some cases, Critical Energy Infrastructure Information (CEII) as defined by the Federal Energy Regulatory Commission (FERC). Sending details asked for in many of the specific questions by electronic means could inadvertently result in the information getting into the wrong hands. Our staff is happy to follow up with yours in a private, confidential setting to discuss these and other questions you may have.

Electric cooperatives have a long, proud tradition of protecting and securing our electric system assets. We are guided by our obligation to serve and the status of our consumers as our owners. The Rural Utilities Service (RUS) has long required each electric cooperative borrower to adhere to rigorous construction standards. Beginning in October 2004, RUS Electric System Emergency Restoration Plan (ERP) regulations in 7 CFR Part 1730 required each borrower to perform a vulnerability and risk assessment and to develop emergency recovery plans regarding physical and cyber incidents. In addition, borrowers are also required to annually exercise their ERP. When disasters strike and electric service is disrupted, cooperatives rely on mutual assistance compacts to deploy teams of line workers across the country to help restore power as quickly and safely as possible. This spirit of cooperation extends to our IOU and municipal counterparts; after Superstorm Sandy, dozens of cooperative crews helped restore power in the Northeast.

Electric cooperatives have participated in each stage of the evolution of the North American Electric Reliability Corporation (NERC), including helping develop Energy Policy Act of 2005 (EPAct '05) amendments to the Federal Power Act which enabled NERC to receive FERC's approval as the Electric Reliability Organization in 2006. Today, numerous electric cooperative technical experts are routinely deployed in NERC teams working on the continual process of writing and improving the already-extensive body of NERC reliability standards, including cyber security standards.

NERC, in a years-long collaborative process with the electric power industry, has produced a body of mandatory, enforceable reliability standards that apply to users, owners and operators of the Bulk Power System. Your letter is particularly concerned with the subset of standards known as the Critical Infrastructure Protection (CIP) standards. To our knowledge, the CIP standards and the Nuclear Regulatory Commission cybersecurity standards are the only mandatory and enforceable cybersecurity standards in place across the vast array of US critical infrastructures. When covered entities are found to have violated the CIP standards, they can be subjected to fines as high as one million dollars per day. NERC has issued sizable fines when entities have been found in violation.

On January 31, 2013, NERC filed its CIP Version 5 standards with FERC for approval. Congressional stakeholders occasionally misunderstand the reasons for having developed multiple versions of the CIP standards in less than six years. NERC and the industry are continuing to address FERC directives, NIST standards and other best practices to make sure the standards evolve with technology and the risks. CIP Version 5 addresses all of FERC's directives and implements key elements of the National Institute of Standards and Technology (NIST) standards.

Electric cooperatives which own or operate Bulk Electric System (BES) assets are required to adhere to one or more of the NERC CIP standards. They have made significant investments in strategic plans, consultants, hardware, software, and full-time employees to ensure compliance and a culture of security at their cooperatives. Electric cooperatives participate in simulations and table-top exercises and NRECA has asked federal government partners to expand these opportunities. However, the electric cooperative network has not simply limited its cybersecurity efforts to a robust, two-way dialogue with NERC and with NERC standards compliance. NRECA and its members (including those cooperatives that are not subject to NERC CIP standards) are engaged in an ongoing conversation with industry and government partners, including FERC, DOE and DHS to increase knowledge of cyber risks and to determine the best means of defense, including implementing appropriate industry best practices.

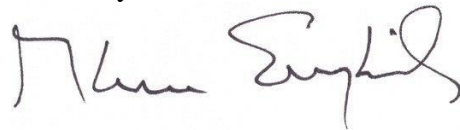
Throughout 2012, NRECA was a leading participant in the Department of Energy's Electricity Sector Cybersecurity Capability and Maturity Model ("Maturity Model" or "Model") development process and several of our members volunteered to host DOE staff for pilots of the Model. The Model presents senior and front-line utility employees with a series of questions and diagnostics concerning cybersecurity. It is now posted publicly and cooperatives continue to work with DOE and industry representatives to expand its use.

The desire to protect our systems has brought NRECA into a partnership with CEOs of the Edison Electric Institute (EEI), the American Public Power Association (APPA) and the Nuclear Energy Institute (NEI) to focus on implementing recommendations of President Obama's National Infrastructure Advisory Council (NIAC). NIAC recommended that the federal government and electric power sector conduct an ongoing, high-level dialogue. The conversation between our associations, the Secretaries of Homeland Security and Energy and White House national security and cybersecurity leadership staff on grid protection has been very productive and is laying the foundation for a functioning public-private working group that can deploy information and instructions across the electric power sector in the event of a severe cyber-attack on the electric grid.

NRECA's Cooperative Research Network (CRN) has been extremely proactive in developing cybersecurity tools targeting distribution utilities (but applicable to utilities of all sizes) which typically are not subject to NERC standards compliance because their operations do not impact the bulk electric system. Since electric cooperatives are at the forefront of smart grid deployment, our members are very much aware of the need to comprehensively address the security of any new telecommunications-enabled devices. As part of its fulfillment of a \$68 million smart grid demonstration program under the American Reinvestment and Recovery Act, CRN developed cybersecurity plans for the 23 participating electric cooperatives. That effort led to the development of a tool that compiles thousands of pages of industry and government guidance on cybersecurity into a digestible, deployable plan. It is publicly available on the web and anecdotal evidence tells us it is in use at many utilities, including some outside the cooperative network. You can download the plan from the web at <http://www.nreca.coop/bestbets/cybersecurity>. CRN now leads training open to all segments of the industry on the plan and cybersecurity best practices.

It has been several years now since the introduction of the House "Grid Act," which NRECA did not support because it sought to centralize authority to write cybersecurity standards within the federal government. The sheer scope of the efforts made by employees and experts in the electric utility field should highlight the tremendous drawbacks to placing the responsibility for writing highly technical standards impacting the generation and transmission of power - our economy's lifeblood - inside the beltway.

Sincerely,

A handwritten signature in dark ink, appearing to read "Glenn English", written in a cursive style.

Glenn English, CEO

Attachment: List of cooperative signatories

Blue Ridge EMC	North Carolina
Brazos Electric Cooperative	Texas
Citizens Electric Corporation	Missouri
East Kentucky Power Cooperative, Inc.	Kentucky
Magic Valley Electric Cooperative, Inc.	Texas
North Star Electric Cooperative	Minnesota
PNGC Power	Oregon, Washington, Idaho, Montana, Wyoming, Utah & Nevada
Seminole Electric Co-op, Inc.	Florida
South Mississippi Electric Power Association	Mississippi
Wabash Valley Power Association	Indiana
Withlacoochee River Electric Cooperative, Inc.	Florida
Wolverine Power Supply Cooperative, Inc.	Michigan