




N A R U C
National Association of Regulatory Utility Commissioners



National Rural Electric
Cooperative Association

A Touchstone Energy® Cooperative 



July 1, 2011

The Honorable Ed Whitfield
Chairman
Subcommittee on Energy and Power
2368 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Bobby Rush
Ranking Member
Subcommittee on Energy and Power
2268 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Whitfield and Ranking Member Rush,

The American Public Power Association (APPA), the Electricity Consumers Resource Council (ELCON), the Large Public Power Council (LPPC), the National Association of Regulatory Utility Commissioners (NARUC), the National Rural Electric Cooperative Association (NRECA), and the Transmission Access Policy Study Group (TAPS) are part of a broad coalition of shared interests within the electric utility sector. That coalition represents the entire body of participants in the North American electric grid. We echo the coalition's strong support for legislation that would strengthen the security and reliability of the electric grid and would protect the bulk power system from cyber attack.

With the Energy Policy Act of 2005 (EPA05), Congress created a system through which the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and utility operators and experts work together to identify and ameliorate cyber vulnerabilities within the bulk power system. Section 215 of the Federal Power Act (which was created by EPA05), allows FERC to approve, remand, or order NERC to write cybersecurity standards to protect the bulk power system from vulnerabilities. Vulnerabilities are potential events which are not accompanied by intelligence that the weakness will be exploited near-term. Section 215 also allows NERC to consult with the utility operators who best understand how any standard they might write would affect grid reliability. This process has evolved since its inception in 2005, and has worked well to harden North American electric systems against persons or entities that would exploit potential gaps in the electric grid for malicious purposes. One of the most beneficial aspects of the process established in EPA05 is the creation of an ongoing dialogue between industry and the federal government on cyber-security issues that can result in modified/updated standards over time to address vulnerabilities.

Chairman Whitfield and Ranking Member Rush

Page 2

June 30, 2011

As the Energy and Power Subcommittee of the House Energy and Commerce Committee moves towards a markup of the Grid Reliability and Infrastructure Defense (GRID) Act of 2011, we urge you to consider changes to the bill that would build upon the existing framework established in EPAct05, while improving upon the ability of the federal government to address emergency situations. The GRID Act acknowledges several challenges facing grid security and makes clear the distinction between threats and vulnerabilities. We applaud Subsection (b)'s grant of new FERC authority to issue emergency orders in the event of a grid security threat. However, we do not support Subsection (c)'s grant of increased authority to FERC to regulate vulnerabilities. The language within this subsection is unnecessary and overly broad. Existing law (EPAct05) already allows FERC to order NERC to issue a standard on any vulnerability FERC might discover. The provision as drafted could allow FERC to rewrite the entire body of mandatory and enforceable standards the electric utility has worked on for nearly eight years (work was being done prior to passage of EPAct05). Also, Subsection (c), if adopted, would allow FERC to enact standards without first consulting with utility experts to determine how the standards could affect grid reliability. Furthermore, any standards written solely by FERC would have no applicability beyond the northern border of the United States. Conversely, the NERC process respects Canadian jurisdictional sovereignty and ensures that standards can be approved by governmental authorities on both sides of the border. Given the integrated nature of the North American grid, a consistent set of standards across the entire system is imperative for achieving robust protection against cyber attacks. Cutting Canadian utilities and authorities out of any grid security process could in fact make the grid less secure.

When the Energy and Power Subcommittee marks up the GRID Act, we urge you to strike Subsection (c). It is important to note that we have strong concerns about other aspects of the GRID Act as currently drafted, including FERC intrusion into regulation of distribution utilities (an area left to states and localities for the last 76 years), insertion of FERC into physical security issues (an area that has been handled for decades by the utilities and local, state and federal law enforcement agencies); and unnecessary language on the Aurora vulnerability. However, with the deletion of Subsection (c), our greatest concern with the bill would be alleviated. Also, we urge you to include NERC in any briefings given to Committee or Subcommittee members on electric grid cybersecurity.

We are available to discuss our concerns further with you or with your staff at anytime. Thank you for your work to enhance the reliability and security of the electric grid.

Sincerely,

The American Public Power Association (APPA), the Electricity Consumers Resource Council (ELCON), the Large Public Power Council (LPPC), the National Association of Regulatory Utility Commissioners (NARUC), the National Rural Electric Cooperative Association (NRECA), and the Transmission Access Policy Study Group (TAPS)

cc: The Honorable Fred Upton

cc: The Honorable Henry Waxman

cc: Members of the House Energy and Commerce Committee