



**Statement for the Record of the
Electricity Consumers Resource Council (ELCON)
Before the House Energy and Commerce Committee
Subcommittee on Energy and Air Quality on
“Protecting the Electric Grid from Cyber-Security Threats”
September 11, 2008**

The Electricity Consumers Resource Council (ELCON) appreciates the opportunity to comment on legislation to protect the electric grid from cyber-security threats. ELCON is the national association of large industrial electricity users. ELCON members are vitally interested in the issue of maintaining the reliability of the bulk power system at all times, including the possibility that the system be subject to cyber-security or other national security threats.

ELCON's members come from virtually every segment of the manufacturing community. As such, they produce not only the goods that are at the core of American life, they also produce goods that are essential to America's national security. ELCON members recognize that an adequate and reliable supply of electricity is absolutely necessary. Accordingly, to promote grid reliability, ELCON was one of the first non-utility participants in the North American Electric Reliability Council (predecessor to today's NERC) as well as an early supporter of creating a federal Electric Reliability Organization (ERO), a role now filled by North American Electric Reliability Corporation (NERC).

ELCON has been working with key industry associations to develop language providing FERC with the authority to respond to imminent cyber-security emergencies. These associations

have produced, and ELCON supports, the proposed draft legislation (herein, the “House discussion draft with the proposed industry language”).

GENERAL COMMENTS

ELCON believes that the best way to address cyber-security matters is through the NERC. Congress authorized the Federal Energy Regulatory Commission (FERC) to approve a fair, open and inclusive organization to develop and enforce standards to assure the reliable operation of the North American grid. Congress added this authority to the Federal Power Act under Section 1221 of the Energy Policy Act of 2005 (EPAct05) creating a new Section 215 of the FPA. FERC certified NERC as this organization. The NERC reliability standard-setting process allows for a balance of interests that ensures access to expertise from industry across the continent for the development of standards with continental application. Section 215 of the Federal Power Act requires FERC approval of any standards before they become mandatory in the U.S.

ELCON is pleased that the House discussion draft makes clear that the NERC standard-setting process remains the appropriate vehicle for developing reliability standards, including cyber-security standards. But ELCON also recognizes that, given the nature of cyber-security emergencies and the need to respond quickly, it makes sense to treat cyber-security standards somewhat differently from operating and planning standards and to allow for quick action to respond to ever-changing threats. Such a process was suggested in a letter forwarded by NERC’s President, Rick Sergel, to NERC’s Board of Trustees and Stakeholders on July 7, 2008. In that letter, NERC suggests the establishment of a task force to “review and where appropriate

recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process.” Importantly, this process would follow the NERC standard-setting model, thereby allowing for the development of cyber-security standards that would be approved by FERC and Canadian governmental authorities. In addition, ELCON is encouraged by NERC's proposals to elevate the profile of its Critical Infrastructure Protection Program, to increase its cyber-security expertise and to better coordinate with governmental authorities. We believe that such steps would allow NERC to better respond to cyber-security issues.

ELCON recognizes, however, that situations can arise that require actions to be taken immediately to avoid grid failures due to cyber-security emergencies. To the extent the current NERC processes are unable to respond to an emergency situation, ELCON agrees that in the U.S., FERC should be able to respond expeditiously to ensure that the grid is protected. The language in the House discussion draft with the proposed industry language would allow FERC to establish interim measures with respect to emergencies identified in the Aurora advisory. However, ELCON believes that such authority must be limited to cyber-security emergencies and must be of a limited duration.

SPECIFIC COMMENTS

- ELCON believes that the applicability of the new provisions should be limited to the “users, owners and operators” of the bulk power system. The practical application of the term “users, owners and operators of the bulk power system” has been developed by NERC in the NERC Compliance Registry Criteria (which has been filed with FERC).

Further, expanding the scope of the new cyber-security legislation to include local distribution facilities would raise serious jurisdictional and implementation issues while not increasing the protection of the grid from cyber-security threats.

- ELCON believes that the applicability of the new provisions should be limited to “cyber-security emergencies.” Other governmental entities have more direct responsibilities relating to other “national security threats.” Further, including such language could spark intense discussions that could delay the enactment of this legislation.
- ELCON believes that the new provisions should require the existence of both (1) a substantial likelihood of a malicious act and (2) a substantial possibility of disruption to the operation of the system for the federal government to conclude that there is a cyber-security threat that would trigger the need for emergency action.
- ELCON believes that the new provisions should contain a “sunset” provision such as that included in Subsection (d) (entitled “Discontinuance”) in the House discussion draft with the proposed industry language.