

NERC Flexible Standards Approval Processes Meet Majority of Grid Challenges

NERC's industry-based and FERC-approved standards development process yields mandatory standards for the bulk power system that are clear, technically sound and enforceable, yet garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cyber-security, through consideration of the National Institute of Standards and Technology (NIST) framework for cyber-security, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also made important revisions to its standards development process by putting in place policies that allow, when necessary, for the confidential and expedient development of standards, including those related to cyber and physical security.

Emergency Cyber Situations Require an Expeditious and Efficient Approach

If the federal government has actionable intelligence about an imminent threat to the bulk power system, the electric power industry is ready, willing and able to respond. We understand it may be necessary for government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards. In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. As FERC, NERC and the electric power industry relationships move forward and mature in the area of reliability and security, any disruption of this would be counterproductive.

Improved Electric Power Industry-Government Partnership with Better Information Flow

In nearly all situations the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system. The electric power industry is fully committed to taking the needed steps to maintain and improve bulk power system reliability and security, and stands ready to work with Congress, FERC, other government agencies and NERC on these critical issues.

Supporting Associations and Contacts:

American Public Power Association	Joy Ditto	jditto@appanet.org
Canadian Electricity Association	Bonnie Suchman	bonnie.suchman@troutmansanders.com
Edison Electric Institute	Scott Aaronson	saaronson@eei.org
Electric Power Supply Association	Con Lass	Class@epsa.org
Electricity Consumers Resource Council	John Anderson	janderson@elcon.org
Large Public Power Council	Jessica Matlock	jdmallock@snopud.com
National Association of Regulatory Utility Commissioners	Charles Gray	cgray@naruc.org
National Rural Electric Cooperative Association	Laura M. Schepis	laura.schepis@nreca.coop
Transmission Access Policy Study Group	Deborah Sliz	dsliz@morganmeguire.com