

Statement for the Record, July 21, 2009 Hearing before the Subcommittee on Emerging Threats,
Cybersecurity, Science and Technology

By the
National Association of Regulatory Utility Commissioners
July 17, 2005
Submitted by
Charles D. Gray, Executive Director

The National Association of Regulatory Utility Commissioners (NARUC) was requested to provide responses to a number of questions presented to NARUC staff by the Subcommittee. The responses provided below are an attempt by the NARUC staff to provide factual responses to the questions posed by the Subcommittee and do not necessarily reflect the official policy positions or views of NARUC and or its membership. We respectfully request that these responses be placed into the record of these proceedings.

What assets do state utility commissioners have jurisdiction over? How does this differ from the jurisdiction of FERC? Is there any cross-over?

The Federal Power Act gives FERC authority over the sale of electricity in interstate commerce (“bulk power”) and interstate transmission. The States retain jurisdiction over unbundled transmission, generation, distribution, and retail rates.

There is some jurisdictional overlap. For example, the States and FERC have concurrent jurisdiction over reliability. Section 215 of the Federal Power Act provides FERC and NERC authority over reliability, but simultaneously asserts that this section does not preempt State authority “to take action to ensure the safety, adequacy, or reliability of electric service within the State, as long as such action is not inconsistent with any reliability standard.” FPA § 215(i)(3). Similarly, transmission tariffs approved by FERC are folded into retail rates.

How does cost recovery work?

Cost recovery is generally established through a rate proceeding whereby a regulatory authority evaluates the costs that the utility requests to recover through rates. These costs may be initiated by the utility, or the utility make seek recovery for investments made in response to a government mandate for something like increased security. Through a rate hearing, the regulatory authority evaluates the requested cost recovery to ensure that the cost conforms to their standards for approving the costs. These standards vary, including evaluations of whether the incurred cost was “used and useful,” “just and reasonable,” or prudently incurred. After evaluating the cost to see if it is recoverable, the regulatory authority generally specifies a mechanism by which the utility will recover the actual cost recovery. Cost recovery mechanisms include base rate changes to tariffs, adjustment clauses, deferral accounts, line item changes, or closed proceedings that allow for the confidential treatment of security costs.

What cost recovery mechanisms exist for utilities to recover costs for physical and cyber security protections?

State regulators are committed to allowing cost recovery of critical infrastructure costs that are prudently incurred. Generally this cost recovery goes through the standard rate case. Regulators have found that the existing inventory of cost recovery protocols and cost recovery mechanisms is sufficient. In some cases, State legislatures have stepped into reaffirm that required security costs are eligible for recovery, as long as the costs are reasonable and prudently incurred.

Does the current FERC/NERC standards-setting process for infrastructure protection (i.e. NERC writes, FERC approves or remands) make sense in a national security context? Does NARUC believe that industry-written standards are appropriate to protect assets as critical to national security as the electric system?

The NERC standards approval process meets the majority of grid challenges. The NERC process engages industry in the development of standards that FERC approves. This process results in mandatory standards for the bulk power system that are clear, technically sound and enforceable, and that garner broad support within the industry. NERC is continually improving its standards; it 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 implemented policies that allow for the confidential and expedient development of standards, including those related to cyber and physical security.

Have any states required utilities to meet physical or cyber security standards that go beyond the NERC mandatory standards? If so, please provide states and standards required.

We are unaware of such State standards, but would be happy to contact our members and get back to you if we learn of any examples.

What are the key aspects of any piece of legislation that seeks to secure the electric grid from cyber and physical attack?

Cyber security legislation should not reinvent the wheel. It should continue to recognize and, if necessary, make more robust the FERC-NERC standards setting process. It should also recognize and respect the power system's existing State and the Federal jurisdictional boundaries.

The legislation should create a framework for improved information flow from the federal government to State regulators and industry of any known threat or vulnerability. This information flow would facilitate increased security for the grid infrastructure. It is critical that any information conveyed from the Federal government to States or industry about a specific threat be timely and actionable to best enable a response. This information can enable a utility's

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.

In the case of actionable intelligence about an imminent threat to the bulk power system, 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 should be the government agency that directs the electric power industry on the needed emergency actions.

Do the commissioners that comprise NARUC maintain any existing authorities that would allow them to require owners and operators of electric facilities to harden their equipment to mitigate the effects of an electromagnetic pulse?

Commission-authorized reliability investments generally require that the utilities protect against “all hazards.” Although Commissions generally do not prescribe against specific threats, “all hazards” standard of review mandates that utilities protect against, or create mitigation measures to limit detrimental reliability effects, from any anticipated threat, including an electromagnetic pulse.

Do the commissioners that comprise NARUC maintain any existing authorities that would allow them to require owners and operators of electric facilities to harden their equipment to mitigate the effects of a cyber attack?

Again, State regulatory authorities generally require utilities to protect against all hazards. NERC sets the cyber security standards. The Commissions, including FERC within its authority over transmission, approve costs based on investments the utilities make to conform to these standards.

How many Smart Grid projects have been funded by commissioners thus far? In general terms, what are the security requirements for these projects?

California and Texas have approved the rollout of advanced metering infrastructure (AMI) with cost recovery. Texas requires that the electric utility have an independent security audit of the advanced meters and report the results of the security audit to the Commission. (*See* Texas Substantive Rule § 25.130, <http://www.puc.state.tx.us/rules/subrules/electric/25.130/25.130.pdf>). I believe that California is still evaluating the rules for the AMI rollout.

There may be additional smart grid projects that have qualified for cost recovery of which we are not aware.

With the rollout of the smart grid investment grants and smart grid demonstration projects under the American Reinvestment and Recovery Act of 2009, there will be a larger number of smart grid projects developed. These funding opportunity announcements discuss and prioritize security, and will certainly be a factor for consideration in the selection of these projects. Smart grid projects, like all projects, must meet NERC’s cyber security requirements. Additional

security requirements and standards are under development. For example, NIST is working to develop cyber security standards for the Smart Grid, with a domain expert working group dedicated to the task. State commission staffs participate in the NIST cyber security working group. State Commission's may choose to adopt and mandate the standards NIST develops for smart grid deployment within its jurisdiction.

Further, NARUC Critical Infrastructure Committee continues to monitor and educate its members on security threats and the evolution of the smart grid.