FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

March 10, 2011

The Honorable Darrell E. Issa
Chairman, Committee on Oversight and
Government Reform
House of Representatives
Washington, D.C. 20515

The Honorable Elijah Cummings
Ranking Member, Senate Committee on Homeland
Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Issa and Ranking Member Cummings:

On behalf of the Federal Energy Regulatory Commission (FERC or Commission), I am pleased to provide a written statement of actions taken in response to the U.S. Government Accountability Office (GAO) report, ELECTRICITY GRID MODERNIZATION: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed (GAO-11-117). I believe that the GAO's recommendations will improve federal/state coordination around cyber security protections for the smart grid and the Commission's cyber security efforts in general.

The report describes the actions of the National Institute of Standards and Technology (NIST) in developing smart grid cyber security guidelines and evaluates FERC's approach for adopting and monitoring smart grid cybersecurity and other standards. GAO explains that FERC has not developed an approach to coordinate with other regulators to monitor whether the electric industry is following the voluntary smart grid interoperability standards it adopts after the NIST actions required by the Energy Independence and Security Act of 2007. The report also identifies key challenges facing the electric industry with respect to securing smart grid systems and networks. These challenges include, for example, that utilities are focusing on regulatory compliance instead of comprehensive security, and that the electric industry does not have an effective mechanism for sharing information on cyber security.

Given the fragmented nature of electricity industry regulation, GAO recommends improved coordination among regulators to help better assess the effectiveness of the voluntary smart grid standards process. Specifically, GAO recommends that the Commission develop an approach to "coordinate with state regulators to (1) periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and (2) develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation." Further, to the extent that the Commission determines that it lacks authority to address any gaps in compliance, GAO recommends that the Chairman

report this information to Congress. The report recommends that the Commission take these same measures with groups that represent municipal and cooperative utilities.

Finally, GAO recommends that FERC, working with the North American Electric Reliability Corporation (NERC) "as appropriate, assess whether any cybersecurity challenges identified in this report should be addressed in commission cybersecurity efforts."

Since the report was issued, FERC has continued meeting with and coordinating with federal and state regulators and other stakeholders to discuss these important matters, and has been considering potential solutions to the challenges posed in the GAO report. Examples of the various actions FERC staff have taken are as follows:

Coordination with Other Regulators

In 2008, the Commission and the National Association of Regulatory Utility Commissioners (NARUC) formed a Smart Grid Collaborative to serve as a forum for federal and state energy regulators to discuss technological and other issues to facilitate the transition to a smart grid. Since then, the Smart Grid Collaborative merged with another NARUC/FERC collaborative focusing on demand response, because many of the topics overlap. The Collaborative provides an opportunity for state and federal energy regulators to discuss emerging issues and to better understand the range of issues that cut across both wholesale and retail energy markets.

Shortly after NIST posted its first five families of interoperability standards last fall, the Commission convened a joint federal-state technical conference to learn about the standards. It was held on November 14, 2010, in conjunction with the NARUC/FERC Collaborative on Smart Response in Atlanta, GA.

As an extension of this existing framework, members and relevant staff of FERC and NARUC met recently to begin a conversation about the recommendations in GAO's report. The report sparked discussion of methods for gathering data, enhancing expertise, and improving communications. Participants at the meeting acknowledged the need for a baseline assessment of utilities' knowledge about smart grid systems and the capabilities and security of equipment that is already deployed. Meeting participants developed several action items to improve communications regarding member regulators' smart grid activities. The discussion also helped to focus plans for future meetings of the Collaborative. Participants anticipate regularly returning to this targeted dialogue about coordinated monitoring and assessment of compliance with standards.

In recent weeks, Commission staff has also met with representatives of the American Public Power Association, which represents community-owned electric utilities, and the National Rural Electric Cooperative Association, representing the interests of cooperatives. The conversations touched on the status of smart grid system deployments and whether cyber security is generally a part of smart grid discussions by municipal and cooperative utilities, helpful resources, and possible opportunities for future discussions and collaborations. Both

organizations agreed that coordination with the Commission once standards are adopted may be useful.

As these discussions continue, the Commission will assess on an ongoing basis whether it has adequate authority to address any gaps in compliance with standards that may jeopardize the cyber security of the transmission grid.

Challenges to Securing Smart Grid Systems

Commission staff has begun analyzing the specific cyber security challenges identified by GAO and whether they should be addressed under the agency's existing cyber security authority and efforts. As background, it may be useful to explain the oversight role of the Commission regarding cyber security of the power grid and our relationship to NERC.

In the Energy Policy Act of 2005, Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is reflected in section 215 of the Federal Power Act. Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The Commission has certified NERC as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States only after Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." The Commission itself does not have authority to modify proposed standards. Rather, if the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter, but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

The Commission's reliability jurisdiction is limited to the "bulk power system," as defined in the Federal Power Act. This term excludes facilities used for local distribution as well as any facilities located in Alaska and Hawaii. The interpretation of "bulk power system" in effect at this time also excludes certain transmission facilities. Under this interpretation, the "bulk power system" excludes virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber security or other national security threats to reliability that involve such facilities and major population areas. It is also important to note that much of the smart grid equipment will be installed on distribution facilities and will not fall under the Commission's Federal Power Act jurisdiction.

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber security. The first versions of the Critical Infrastructure Protection (CIP) standards were received from NERC, as the Electric Reliability Organization, in late 2006. The Commission directed NERC to make numerous changes to the standards in order to improve the cyber security protections within those standards. These directives, if implemented, would help to address some of the concerns in the GAO report. While there have been incremental updates to the CIP standards, there are still many outstanding directives that have not been incorporated into the latest versions. The Commission will continue to work with NERC and the industry within the limitations of our authority to oversee their efforts to incorporate these directives into the standards.

Beyond that role, staff has begun considering potential solutions to the challenges identified in GAO's report and ways to address those challenges, including coordination with other federal agencies and initiatives and outreach to industry organizations. In addition, these challenges might implicate Commission interactions with and directions to NERC. Deliberation of the best ways to proceed is ongoing within the Commission.

Staff also arranged a briefing by the National Electric Sector Cybersecurity Organization (NESCO), which is an independent program aimed at enhancing the integration of grid technologies so that they are adequately protected against cyber attacks. The briefing focused on information sharing for the electric sector. Staff learned about NESCO's various tools and outreach programs focusing on coordination among cyber security experts within the electric sector. Commission staff believes these education and coordination activities have the potential to address some of the cyber security challenges facing the electric industry, and staff will continue to follow NESCO's activities. Staff is also conducting outreach to other organizations and stakeholders with relevant expertise in the interest of identifying other steps that may address cyber security challenges like those discussed in GAO's report.

In addition, Commission staff recently convened a second technical conference on January 31, 2011, and solicited written comments to aid the Commission's determinations regarding adoption of smart grid standards, processes leading to and attributes of consensus, and smart grid benefits that standards should enable. Feedback following that technical conference is expected to inform the Commission's cyber security efforts, in addition to its rulemaking activities.

The Commission appreciates this opportunity to share its reactions to GAO's report and its approach for future actions. If you have any questions, please contact Mr. Leonard Tao, Director of the Office of External Affairs, at (202) 502-8214.

Sincerely,

Jon Wellinghoff
Chairman

Document Content(s)