FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

February 14, 2012

The Honorable Daniel K. Inouye
Chairman, Committee on Appropriations
United States Senate
Washington, D.C. 20510

The Honorable Thad Cochran
Ranking Member, Committee on Appropriations
United States Senate
Washington, D.C. 20510

Dear Chairman Inouye and Ranking Member Cochran:

On behalf of the Federal Energy Regulatory Commission (FERC or Commission), I am pleased to provide a second 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); an initial statement was provided on March 10, 2011.

The GAO report described the actions of the National Institute of Standards and Technology (NIST) in developing smart grid cyber security guidelines and evaluated FERC's approach for adopting and monitoring smart grid cyber security and other standards. GAO explained that FERC had not developed an approach to coordinate with other regulators to monitor the extent to which the electric industry follows any voluntary smart grid interoperability standards it adopts after actions taken by NIST in accordance with the Energy Independence and Security Act of 2007. The report also identified key challenges facing the electric industry with respect to securing smart grid systems and networks. These challenges include, for example, that the current regulatory environment leads to a lack of clarity about the division of responsibility between federal and state regulators, making it difficult to ensure the cybersecurity of smart grid systems, and that regulatory bodies may not be able to respond to rapidly evolving cybersecurity threats. Additionally, GAO expressed concern that utilities are focusing on regulatory compliance rather than comprehensive security, and that security features are not consistently built into smart grid devices.

Given the fragmented nature of electricity industry regulation, GAO recommended improved coordination among regulators to help better assess the effectiveness of the voluntary smart grid standards process coordinated by NIST. Specifically, GAO recommended 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 recommended that the Chairman report this information to Congress. The report also

recommended that the Commission take these same measures with groups that represent municipal and cooperative utilities.

Finally, GAO recommended 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."

Subsequent to our initial statement of action prepared in March of last year, FERC issued an order declining to institute a rulemaking proceeding to adopt specific interoperability standards. Applying the "sufficient consensus" test specified in the relevant statute, the Commission determined that there was insufficient consensus to institute such a proceeding at that time. Since then, Commission staff have continued meeting with state regulators and other stakeholders to discuss the interoperability framework process, and staff have been considering potential solutions to the challenges posed in the GAO report, as discussed below.

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.

The Commission's approach has been to work collaboratively with state regulators and NIST. We continue to have a formalized process with NARUC (the Smart Response Collaborative) where monitoring for compliance and discussing any gaps in compliance, among other relevant issues, can be done in conjunction with state regulators. Considering the continuing evolution of standards and the lack of sufficient consensus for regulatory adoption, however, Commission staff believe that coordinated monitoring of compliance with standards would be premature at this time. This may change as new standards are developed and deployed in industry. With regard to NIST's interoperability framework process and its cybersecurity guidelines, Commission staff continue to follow the development of standards and are available to advise both FERC and state commissioners and/or staffs upon request.

As developments continue, the Commission will assess on an ongoing basis whether it has adequate authority to address any gaps in compliance with adopted standards that may impede achieving an interoperable and secure electricity system.

Challenges to Securing Smart Grid Systems

Commission staff have continued to analyze 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 codified in section 215 of the Federal Power Act. Section 215 states the Commission may certify 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 by virtue of NERC's definition of the "bulk electric system" 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, including Version 4 of the standards which is currently pending before the Commission, 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.

The Commission has addressed several of the challenges identified by GAO in carrying out other responsibilities in recent months. The Director of the Commission's Office of Electric Reliability in recent testimony before Congress discussed current limitations in Federal authority to protect the grid against physical and cyber threats. Office Director Joseph McClelland testified before committees of the House of Representatives and Senate that the Commission's current legal authority is inadequate

to protect against entities intent on attacking the United States through vulnerabilities in the electric grid. He stated that, although NERC's standards development process can address routine reliability matters, it is too slow, too open and too unpredictable to ensure responsiveness in cases where national security is endangered and circumstances require urgent action. He stated, among other things, that any new legislation should allow the federal government to take action before a national security incident has occurred, enabling the federal government to require mitigation before or while NERC and its stakeholders develop a standard.

One existing mechanism that allows sharing of threat information and voluntary mitigation is NERC's alert process. The Commission, its federal partners, and NERC often discover, identify or receive information that is critical to protecting the reliability of the bulk power system in North America. NERC develops an alert with the support of subject matter experts; the Commission can propose edits for the alerts, but NERC is not required to accept them. Any federal agency can work with NERC on these alerts including the Commission, the Department of Homeland Security, the Department of Energy, the Nuclear Regulatory Commission, the Federal Bureau of Investigation, and others in the intelligence community to quickly advise the electric industry of threats on a non-classified level and to help NERC develop guidance on protective actions and security practices for industry's consideration. These advisories are not mandatory or enforceable and cannot substitute for standards, but they permit information on threats and vulnerabilities to be disseminated quickly. In addition, Commission staff actively coordinate with these same agencies to monitor threats and vulnerabilities. The information is then provided to the private sector to raise awareness of these threats and vulnerabilities and to encourage them to take proactive action against them.

Regarding a lack of clarity about the division of responsibilities between federal and state regulators, the Commission last year directed NERC to revise its definition of the bulk electric system in several ways, which may help to clarify the boundaries between federal and state responsibilities. In particular, the Commission indicated that the new definition should ensure that certain facilities that are necessary to operate the bulk electric system reliably are subject to NERC's mandatory rules while continuing to observe Federal Power Act section 215 statutory boundaries that exclude the local distribution system from Commission jurisdiction. This order was done through a rulemaking and the Commission received and considered the comments of the stakeholders including those of individual states.

Responding to the concern that utilities focus on regulatory compliance rather than comprehensive security, Commission staff have begun conducting performance audits in addition to traditional compliance audits. These performance-based assessments evaluate the robustness of utilities' security postures and offer suggestions beyond mere compliance. Moreover, these audits are used to promote industry best practices in order to minimize potential vulnerabilities, raise security awareness, and strengthen cyber defense-in-depth policies and procedures. During such an audit, Commission staff will also review the actions utilities have taken regarding the NERC alerts.

I appreciate this opportunity to share a summary of the Commission's actions relevant 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

cc:

Senator Dianne Feinstein,
Chair, Subcommittee on Energy and Water Development

Senator Lamar Alexander
Ranking Member, Subcommittee on Energy and Water Development

Senator Joseph I. Lieberman
Chairman, Committee on Homeland Security and Governmental Affairs

Senator Susan M. Collins
Ranking Member, Committee on Homeland Security and Governmental Affairs

Senator Jeff Bingaman
Chairman, Committee on Energy and Natural Resources

Senator Lisa Murkowski
Ranking Member, Committee on Energy and Natural Resources