FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

Mr. Ricky R. Hass
Deputy Inspector General for Audit Services
Department of Energy
1000 Independence Ave., S.W.
Washington, DC 20585

Dear Mr. Hass:

Thank you for providing the Department of Energy Inspector General's draft report on the audit of the Federal Energy Regulatory Commission's (FERC) Monitoring of Power Grid Cyber Security dated November 16, 2010. I appreciate the opportunity to respond to the draft findings and recommendations.

In Order No. 706, FERC approved the Critical Infrastructure Protection (CIP) standards, the first set of mandatory cyber security standards for the bulk electric system. The CIP standards were developed by the North American Electric Reliability Corporation (NERC) through its stakeholder process. Under section 215 of the Federal Power Act (FPA), FERC lacks the authority to develop or modify reliability standards on its own: FERC can only approve or remand standards that are developed by NERC. When approving a standard, FERC can also direct NERC to develop changes while the approved version is in effect.

Though Order No. 706 approved the CIP standards, the 214-page order directed NERC to make significant improvements, including to increase the level of cyber security reflected in the requirements and to provide greater clarity and guidance to industry. Since Order No. 706 issued in January 2008, FERC has monitored NERC's initiatives and has even actively engaged in its process to implement these directives to improve the CIP standards so as to minimize the threat to the bulk electric system posed by cyber attacks. Despite work to date to improve the CIP standards, FERC believes that effective cyber security standards cannot be developed at the pace recommended in the draft audit report under the existing statutory framework.

While the NERC standards development process is appropriate for most reliability standards, cyber attacks are qualitatively different from other reliability problems: they may be covert and coordinated, use previously unknown vulnerabilities and exploits, and emerge with alarming speed. Although cyber security requirements developed under the reliability standards might address some threats, they simply cannot completely eliminate them. To quickly, comprehensively, and effectively respond to cyber security threats, FERC requires additional authority. Indeed, only with additional authority is it possible to achieve the cyber security objectives in the draft audit report's Recommendation Nos. 2 and 3. Separately, FERC concurs with Recommendation Nos. 1, 4, and 5 and is taking steps to implement them.

Response to Findings

As discussed in the attachment, the draft audit report contains findings that are unsupported or run contrary to the facts or applicable legal standards. For example:

- The draft audit report criticizes FERC's decision to approve the CIP standards knowing their deficiencies. However, the report does not appreciate that prior to their approval, there were no mandatory reliability standards at all for cyber security. As FERC stated in Order No. 706, this first set of CIP standards represented a "baseline" and FERC concurrently directed substantial and numerous modifications to the standards as they were approved. As a result of these directives, FERC received numerous comments from industry objecting on the grounds that it had overstepped its authority by being overly prescriptive. Lastly, the statutory reference to remanding standards is based on section 215(d)(2) of the FPA, which limits FERC's review of standards to a determination of whether they are "just, reasonable, not unduly discriminatory or preferential, and in the public interest." FERC cannot reject a standard unless the proposal fails the statutory test. The draft audit report does not conclude that the statutory test was not met.

- The draft audit report is critical of the pace of the original development and implementation of the CIP standards. However, the report minimizes the complexities inherent in imposing, for the first time, mandatory cyber security standards on the diverse entities that make up the users, owners, and operators of the bulk electric system. FERC shares the concerns in the draft audit report regarding the development of the CIP standards; however those concerns are largely a function of the statutory framework in which FERC and NERC operate.

The attachment contains a detailed response to these and other findings for which FERC believes there is inadequate support in the draft audit report or for which additional information should be considered.

Response to Recommendations

1. Continue to work with Congress to obtain authority appropriate for ensuring adequate cyber security over the bulk electric system.

FERC continues to seek authority appropriate for ensuring adequate cyber security over the bulk electric system. As noted in the draft report, FERC officials have testified before Congress repeatedly to request additional authority over cyber security standards. FERC plans to continue its efforts to obtain the necessary authority.

2. Work with NERC to continue refining the CIP standards to include risk-based requirements and cyber security controls that keep pace with emerging threats and help minimize vulnerabilities to the power grid.

While FERC continues to work with NERC to improve the CIP standards, the current statutory framework is inadequate for addressing emerging cyber security threats through mandatory standards and minimizing vulnerabilities to the power grid. FERC believes that additional authority, consistent with the first recommendation, is necessary to address cyber security threats in a timely and comprehensive manner. FERC has repeatedly asserted through Congressional testimony and public statements that the section 215 process is slow, not confidential, and not necessarily even responsive to FERC's directives– all of which make it ineffective against threats to national security that are propagated through cyber security attacks on the power grid.

3. Ensure timely development and approval of the CIP standards, as practical, including increasing communication with NERC and electric industry entities during the process.

FERC makes every effort, consistent with its statutory obligations, to approve CIP standards as soon as possible after they are developed by NERC. Moreover, FERC routinely engages in open communication with NERC and industry through NERC's standards development forums, technical conferences, seminars, and many other forms of dialogue. However, FERC's existing authority limits its influence over the development of CIP standards because only NERC, through a stakeholder controlled process, can propose and modify standards. Again, FERC believes that additional authority, consistent with the first recommendation, is necessary to address cyber security threats in a timely and comprehensive manner.

4. Ensure the Commission adequately monitors the performance of NERC and the eight regional entities responsible for security over the bulk electric system.

Pursuant to its statutory authority, FERC regularly participates in audits performed by NERC and the Regional Entities, which include cyber security reviews, to assure compliance with the standards. FERC directed in a January 2009 order, and urged during audits and in subsequent feedback to the Regional Entities, that areas of concern that are not yet violations be included in the reports that are issued after a Compliance Audit or Spot Check. FERC also continues to examine the allocation of staff and budget allocated to CIP standards compliance activities both as a part of the routine budget submittals to FERC as well as in other FERC oversight activities.

5. Ensure that cyber security performance metrics for NERC and its regional entities are developed and utilized that enable the Commission to effectively monitor and assess program performance.

FERC is aware of and is working in conjunction with NERC and its Regional Entities to develop meaningful metrics to assess and monitor program performance. This collaboration effort has been on-going for a number of years.

I appreciate the efforts made by the audit team in preparing the draft audit report and for its recommendations. Consistent with the recommendations, FERC will continue to use its current statutory authority to protect the bulk electric system from cyber security threats while pressing for additional authority to respond to these emerging threats more effectively.

Sincerely,

Jon Wellinghoff
Chairman

Attachment