April 28, 2009

The Honorable Edward J. Markey
Chairman
Subcommittee on Energy and Environment
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am writing in response to your letter of April 9, 2009 regarding the threat of cyber attack to our Nation's electricity infrastructure. I share your concern regarding the importance of maintaining the security of the electric grid from cyber attack. It is crucial that the electric grid be protected from entities that may seek to disrupt the supply and distribution of electricity within the United States. The Commission is committed to exercising all of the authority that Congress has given it to help protect the power grid. However, Congress needs to be aware that the Commission's current authority is not sufficient to ensure the cybersecurity of the grid. The existing process is based on industry consensus and is, therefore, too slow, subject to disclosure to potential attackers, and not responsive enough to adequately address matters that affect national security.

The Energy Policy Act of 2005 (EPAct 2005) authorized the Commission to approve and enforce mandatory reliability standards, including cybersecurity standards. Under this framework, reliability standards are developed and proposed by the Electric Reliability Organization (the North American Electric Reliability Corporation or NERC) for the applicable users, owners, and operators of the bulk-power system (which excludes significant areas and facilities within the United States).

The NERC process is open and inclusive, requiring that NERC post not only the standard under development, but all public comments as well as the rationale used to justify its development. The progress of a draft standard is controlled by the ballot body; NERC's rules provide that NERC cannot approve it until after a two-thirds majority of a quorum of the ballot body members (*i.e.*, the industry stakeholders) vote to approve the standard. Only after a standard passes these hurdles (which typically takes years) can the NERC Board of Trustees consider and approve the standard and then file it with the Commission for review. The Commission cannot modify proposed standards if it deems them inadequate, but can only remand them back to NERC. As you note in your letter, the Commission has reviewed and approved NERC's first set of eight cybersecurity-related reliability standards, but has also directed NERC to work on modifications to

them. These modifications are critical to improving the standards so that they will better protect the bulk power system from malicious cyber attacks. The process of modifying and improving the standards is ongoing.

The Commission will review any revisions to the cybersecurity-related reliability standards as soon as they are filed by NERC. It is important to note that although the Commission has directed that NERC work on modifications to the cyber standards, any such modifications are subject to the same standards development process described above (including the requirement for a two-thirds majority vote) and may, therefore, result in proposed standards that do not address the Commission's directives. Such an event may result in either further directives by the Commission for modification or possibly a remand (rejection) of the proposed standards, thereby further delaying the implementation of cybersecurity requirements. Once the standards are approved by the Commission and subsequently implemented by the regulated entities, the Commission will work to ensure full compliance in the industry.

The actions that the Commission has taken to approve reliability standards provide an initial foundation to help protect the security of the electric grid. However, as noted, significant improvements are needed. Further, I remain concerned that certain evolving threats and vulnerabilities will not be mitigated by the existing standards. In short, the Commission does not have authority to modify deficient standards presented to it by NERC, to ensure that the standards under development by NERC will be responsive to the Commission's directives, or to secure sensitive grid information from disclosure. It also does not have authority to direct immediate action in emergency situations to secure the electric grid. The ability of the Commission to respond to emergencies is crucial to ensuring the cybersecurity of the power grid.

The Commission looks forward to working with the Congress in this area to improve the security of our electric grid. Please let me know if you have any further questions or concerns.

Sincerely,

Jon Wellinghoff
Chairman

Enclosure

Responses to Questions from 4/9/09 Letter to Chairman Wellinghoff:

1. *What is the Commission's view of the results of the North American Electric Reliability Corporation survey? What percentage of Critical Cyber Assets have been identified? What is the significance of the information backbone of the electric grid being compromised? What immediate steps is the industry taking to stop these breaches?*

The survey results are of significant concern. When the Commission approved the Critical Infrastructure Protection (CIP) cybersecurity standards, it found that they allowed significant discretion for the regulated entities to decide whether their equipment should be considered "critical cyber assets" and thus subject to the standards. To address this issue, the Commission directed NERC to modify the standards to include a mechanism for external review and approval of critical asset lists. The Commission described such a review mechanism as providing timely, comprehensive guidance to entities on the adequacy of their critical asset lists. These directives are currently being considered in NERC's standard development process and are expected to be reflected in modified standards. I would like to clarify, however, that although NERC's survey results are an important and useful metric in an ongoing process of improving the cybersecurity of the electric grid, more data and analysis is needed to understand the implications of the survey. For instance, the survey gave small entities the same weight as large entities with many more generation units. Therefore, when NERC stated that only 29% of generation owners and generation operators reported at least one critical asset, it is unclear what portion of the Nation's generation capacity that 29% represents, or what portion the designated critical assets represent. Thus, it is not clear what percentage of critical cyber assets have been identified but it is clear that this issue is serious and represents a gap in cybersecurity protection.

I believe that the information backbone of the electric grid is essential to the reliable and efficient operation of the bulk-power system. Protecting the electric grid from cyber intrusions is critical to ensuring electric service to our citizens, industry and the military. Interruption of this service through a cyber attack on the information and control backbone of the electric grid, represents a threat to the health and safety of our citizens, our economy and our national defense.[1] The electric industry is currently working to reach compliance with the CIP standards. However, additional work will be needed to ensure the security of the grid. The Commission's order approving the CIP standards, Order No. 706, requires NERC to make significant modifications to the standards and to develop guidance on how they should be implemented. That work is

[1] As an example, a February 2008 Defense Science Board report entitled "More Fight – Less Fuel" concluded that "…critical missions at military installations are vulnerable to loss from commercial power outage and inadequate backup power supplies."

underway but will take significant time to complete. Compliance monitoring and enforcement of the standards will also be an important and constant effort which will identify any shortcomings in implementation steps. This is an ongoing process that is in its starting phase.

2. *If foreign nations or hostile groups already have gathered detailed information to develop a "map" of the electricity grid, what actions can be taken now to prevent this information from being used to attack the grid?*

By itself, a "map" of the electric grid is insufficient to allow outsiders to attack the grid. Attackers must also be able to gain access to controls over the grid, through cyber manipulation or other methods. Accordingly, the key to preventing an attack on the electric grid is denying potential attackers access to critical controls. Such an attack could involve either or both physical access or electronic access. The CIP standards promulgated by NERC and approved by the Commission, subject to future modifications, are a first step to address both physical and electronic access to cyber assets. However, the Commission needs additional authority to ensure that, in the event of an imminent national security threat, targeted or mapped entities take timely and effective actions to protect the power grid from vulnerabilities and threats that endanger national security. It is important that if this authority is conveyed, it include the ability of the Commission to protect information regarding the vulnerability or threat as well as to protect the individual cyber configurations and mitigation plans of the affected entities.

In many ways, electronic access to the grid is most worrisome since an attacker could obtain electronic access from outside of the United States, making the number of potential attackers much larger and the personal risk to the attackers much less. However, significant threats exist from both physical and electronic access, and both areas must be addressed in protecting the grid. A range of techniques can be used to reduce the risk of cyber attacks, including steps as obvious as using frequently changed complex passwords and more involved steps such as adding electronic gateways and multi-factor user authentication.

3. *Have the CIP standards been fully implemented by industry? If not, why not?*

The implementation process for the CIP standards is currently ongoing, and is not yet fully complete. According to the plan developed in the NERC standards development process and approved by the Commission in January 2008, different parts of the CIP standards must be completed by different types of entities (e.g., transmission operators versus generation operators) at different dates. With a few exceptions, all entities are to be compliant with all of the CIP standards by the end of 2009.

4. *Are the current "CIP" standards sufficient to prevent cyber-security attacks and to respond to breaches? In not, what additional standards are needed?*

No. In Order No. 706, the Commission found that the CIP standards as presented by NERC needed substantial improvement and thus the Commission required modification of the standards. As has been discussed before, the efficacy of the modified standards that industry proposes to the Commission will depend on how well the NERC drafting team responds to the directives of the Commission and on the willingness of industry to approve the modified standards in the NERC balloting process. In addition, the types of threat (such as new viruses) as well as the attack mechanisms (such as through wireless communications) are constantly changing. Although the standards are expected to evolve and continue to improve over time, they cannot be expected to address sophisticated, fast-moving, and targeted threats that may compromise national security. Assuming the CIP standards are modified in a manner that is acceptable to the Commission, it is still likely that additional standards will be needed in the future to address these evolving threats. I am not able at this time to describe the nature of the additional standards that may be required.

5. *Has FERC developed metrics to measure the efficacy of the CIP standards? If so, what are these metrics? If not, why not?*

No, the Commission has not yet developed metrics to measure the efficacy of the CIP standards. As noted above, the Commission reviewed the expected efficacy of the current CIP standards in Order No. 706 and immediately ordered NERC to develop substantial modifications. Only after NERC completes the modifications to the standards and files them for the Commission's approval can the Commission approve them and measure their efficacy, or alternatively decide to remand them or order further modifications to the standards. During the interim period while NERC is working on the modifications the Commission has directed, the Commission will work with NERC to ensure compliance with the existing standards and review periodic audits and vulnerability assessments. Gathering meaningful metrics on cybersecurity will likely involve very sensitive security data and, without additional authority, the Commission may need to limit its collection of information to protect such information from public disclosure. To some degree, FERC can avoid this risk by inspecting documents without compiling them, but this is a very cumbersome process that limits the ability to collect and identify metrics information.

6. *What processes are on-going at NERC to identify the need for new cyber-security standards?*

The Commission is aware of several NERC processes to evaluate the CIP standards and determine whether new standards are necessary. For example, in Order No. 706, the Commission directed NERC to consider the effectiveness of the

cybersecurity standards promulgated by the National Institute of Standards and Technology (NIST) by interviewing entities that are subject to both the CIP standards and the NIST standards, such as TVA. Additionally, NERC will conduct compliance audits, detailed incident reporting, and vulnerability assessments designed to identify shortcomings in cybersecurity standards and the need for new or modified standards. All of these methods will be part of the CIP standards compliance and monitoring processes once all entities are required to be compliant with the standards and are expected to help inform NERC about the need for new or revised requirements.

7. *Is too much discretion given to industry participants in creating the cyber-security standards, since two-thirds of the group's members must support a standard before it is adopted or modified?*

It is correct that the existing standards development process requires two-thirds of the balloting body to approve a standard before it can be submitted to the Commission. For the previously stated reasons, this process is not suitable to address matters that implicate national security interests, particularly when information regarding a threat or vulnerability is classified or restricted and all balloting body members may not have access to it. The two-thirds voting requirement could affect the development of standards in at least two ways. The first is during the posting, commenting and balloting process. If a standard is considered undesirable to one-third of the industry, those stakeholders can either attempt to have the standard revised during the process, or reject it in balloting. Second is the influence that the two-thirds requirement has on the drafting process. Drafting team members are well aware of the voting requirement and that a well-written standard that is not adopted by industry is of little value. Accordingly, the two-thirds requirement may impact the quality of the standards submitted even before industry votes.

8. *What authorities does FERC possess to prevent and respond to cyber-security threats and breaches? Does FERC need additional authorities to protect the electricity grid from those threats?*

The Commission's role is limited. In August 2005, Congress enacted Federal Power Act section 215, which entrusted the Commission with a major new responsibility to oversee the development of mandatory, enforceable reliability and cybersecurity standards for the bulk-power system. The Commission-certified Electric Reliability Organization (ERO), NERC, is responsible for proposing, for Commission review and approval, reliability and cybersecurity standards or modifications to existing reliability and cybersecurity standards to help protect and improve the reliability of the Nation's bulk-power system. As noted above, the Commission may remand a deficient standard to NERC for modification or approve a standard with directions to NERC to work on further improvements to the standard. It may also on its own motion direct NERC to develop a standard on a particular matter. However, the Commission has no authority

itself to modify standards presented by NERC or to establish standards it concludes are necessary to address a vulnerability or threat.

The Commission also has a role under Section 1305 of the Energy Independence and Security Act of 2007 to work with NIST to develop and approve standards and protocols necessary to ensure smart-grid functionality and interoperability. Once sufficient consensus is reached by NIST participants, the statute requires FERC to institute a rulemaking to adopt standards. These standards and protocols can play an important role in helping to protect both the reliability and cybersecurity of the grid. However, it is important to note that there are questions regarding the Commission's authority to enforce these standards with respect to all of the entities that will be using and operating the smart grid.

As has been explained in response to prior questions, although the Commission has been diligent in carrying out its responsibilities under its current authority, I believe that the Commission needs additional authority to respond to immediate threats to the electric grid. When faced with a cyber security or other national security threat to reliability, the Commission may need to act decisively in hours or days, rather than wait for the NERC process, which typically takes multiple years. Although NERC has an expedited process, that expedited process has never been used, and even the expedited process is not likely to allow a timely, adequate response to an imminent threat. For example, if the NERC process results in a standard that does not address the threat, the Commission has no authority to modify the standard and would be limited to remanding it back for unlimited additional "expedited" processes, leaving the grid vulnerable in the meantime. Thus, the Commission's current authority is not sufficient to ensure timely action to protect the grid. Additionally, the open, inclusive NERC procedures could result in wide publication of the vulnerability and potential solutions before adequate mitigation measures are implemented.

Accordingly, authority should be granted to the Commission, following a directive or determination by the President of an imminent national security threat to reliability, to order such emergency measures or actions as are necessary to protect the reliability of the bulk power system. This authority should encompass both physical and cyber security, as threats to the grid exist in both areas. Additionally, the Commission must have the ability to protect security-sensitive information from public disclosure. The potential for publication of sensitive information regarding cyber threats and other threats to the security of the grid both weakens the Commission's ability to respond to cyber threats and endangers compliance by private entities concerned about the sensitivity of information they provide to the Commission.

Although I believe that such an expansion of Commission authority is necessary and would help protect the electric grid, it is important to note that protecting the "bulk-power system" from threats does not address two important areas where threats may also

exist. First, areas such as Alaska and Hawaii are not defined as part of the bulk-power system but are also vulnerable to cyber attack. Second, the term "bulk-power system" is generally defined as transmission facilities in excess of 100 kV, although it is subject to the individual interpretations of the NERC regions. This discretion has been the subject of concern and inquiry by the Commission in the Northeast as some major facilities in that region (including those that serve New York City) have been excluded from coverage under the reliability standards.