FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

11-13-07A11:13 RCVD

November 9, 2007

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats,
Cybersecurity, and Science and
Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security
And Infrastructure Protection
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your letter of October 17, 2007, regarding a recently-identified cyber vulnerability that could affect the electric infrastructure of the United States. I share the Subcommittee's concern that all appropriate steps be taken to protect against actions that potentially could cause widespread and long-term damage to the nation's electric infrastructure and, in turn, significantly impact our economy, public health and national security. Also, I want to thank the Subcommittee for the opportunity to have Mr. Joseph McClelland, Director of the Federal Energy Regulatory Commission's (Commission) Office of Electric Reliability, testify at your hearing. Yours was an important and successful hearing, and your Subcommittee should be congratulated for drawing attention to this issue.

The Commission is taking action to protect against cyber threats. As discussed below, the Commission is moving forward with respect to its rulemaking to establish mandatory cyber security (Critical Infrastructure Protection, or CIP) standards for the bulk power system. The Commission is also taking steps to confirm what mitigation actions generation and transmission owners and operators already have taken, or intend to take, to protect against this specific cyber vulnerability. The Commission takes seriously its responsibility to ensure that appropriate requirements are in place to provide for

reliable operation of the bulk-power system and, depending on what we learn with respect to actual mitigation efforts, we will consider additional steps as appropriate within our statutory authority.

As an initial matter, it is important to review the statutory and regulatory framework in which mandatory reliability standards are developed and approved. The Energy Policy Act of 2005 (EPAct 2005) provided the Commission new authority, under section 215 of the Federal Power Act, to require users, owners, and operators of the bulk power system to comply with reliability standards proposed by the Electric Reliability Organization (ERO) and approved by the Commission. Pursuant to section 215 and the Commission's implementing regulations, the ERO (North American Electric Reliability Corporation or NERC) conducts an open and inclusive process to develop new or modified standards and solicits comments from all interested persons and groups on those standards prior to submitting them to the Commission.

Once proposed standards are submitted to the Commission, the Commission determines whether they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission may approve a standard if it complies with the statutory test or can remand the standard to the ERO if it does not. The Commission also has the authority to direct the ERO to develop a new or modified standard through an ERO standards development process. The Commission does not, however, have authority under section 215 to either revise a proposed standard or establish a new standard that has not gone through some type of ERO-administered process that complies with the basic statutory requirements of section 215. Moreover, unless a reliability standard has been approved by the Commission pursuant to the section 215 statutory framework, it is not mandatory or enforceable under section 215.

Your letter specifically references NERC's proposed CIP standards which are pending before the Commission. NERC submitted these proposed standards on August 28, 2006, and requested that entities begin compliance no earlier than mid-2009, with full compliance being achieved by the end of 2010. The Commission issued a staff report on December 11, 2006 identifying significant concerns regarding the CIP standards and sought public comment on staff's concerns. As a result of this report, 38 commenters filed approximately 400 pages of comments. After reviewing and considering the comments, the Commission then issued a notice of proposed rulemaking on July 20, 2007 and although the Commission has proposed to approve the standards as a first step, it has also proposed that NERC develop and submit to the Commission many significant revisions to the standards to make them more effective. Pursuant to the earlier point concerning the revision of existing standards, however, these changes will not be immediately implemented as they will have to be developed through the ERO's standards development process and subsequently re-submitted to the Commission for review before they can be approved and subsequently made mandatory. Approximately 69 comments

comprising over 800 pages have been filed on the proposed rule and the Commission anticipates issuing a final rule in the near future.

Your letter also references the fact that NERC, acting through its Electric Sector Information Sharing and Analysis Center (ES-ISAC), issued an advisory on June 21, 2007, describing mitigation measures intended to reduce the risks associated with the identified cyber vulnerability. You also note that the Commission in a recent order held that NERC lacked authority under section 215 to require specific action other than in circumstances involving a violation of a Commission-approved reliability standard.

I appreciate the opportunity to address this concern. The Commission so held because Congress, in enacting section 215, did not give NERC, or even the Commission, the authority to impose mandatory standards that have not gone through a standards development and approval process consistent with section 215. The Commission is an agency of limited powers and we only have the tools Congress has given us. Moreover, we have no legal authority to delegate power to NERC that we ourselves do not possess. In its filing, NERC sought authority to require certain actions outside the section 215 process, but failed to identify any legal authority upon which it could require actions that were not compelled by an approved reliability standard. Despite this, the Commission agreed with NERC that it may issue alerts and recommend action whenever it believes corrective actions may be necessary. In fact, the Commission encourages such action and recently directed NERC to follow each such alert or recommendation with a report to the Commission on the level of compliance no later than 30 days from the date on which NERC requests action. Such reports will help the Commission determine if further action is needed.

You express concern that, because the CIP standards have not become mandatory, NERC has no authority to require compliance with its advisory. It is important to point out that, while the Commission has proposed that the CIP standards be strengthened significantly and intends to finalize its rulemaking in the near future, the CIP standards as proposed by NERC in fact do *not* require the specific mitigation actions that are discussed in your letter or referenced in the ES-ISAC advisory. Therefore, the fact that the CIP NOPR remains pending does not affect whether the advisory is mandatory.

I agree with your letter that it is important to assess compliance with the ES-ISAC advisory. To determine the level of compliance and the effectiveness of such compliance, the Commission therefore intends to issue an order directing submission of certain cyber security information from each generator owner and operator and transmission owner and operator in the United States registered by NERC. As a first step toward that end, the Commission, in an October 23, 2007 letter, informed the Office of Management and Budget (OMB) of the Commission's intended action, and requested OMB's emergency approval of the Commission's information collection request. This emergency approval, if granted, would expedite the OMB approval process, which in

ordinary circumstances allows a sixty-day comment period on the proposed information collection before OMB approval. A copy of the Commission's October 23, 2007 letter to OMB is enclosed.

NERC, following the Subcommittee's October 17, 2007 hearing, issued a survey regarding mitigation efforts, with responses due on November 2, 2007. Although we support NERC taking the actions it believes are necessary as ES-ISAC, we do not believe NERC's survey provides sufficient information for the Commission to determine whether further action is appropriate. For example, it does not provide information on what facilities are the subject of the mitigation plans, what steps to mitigate the cyber vulnerability are being taken, when those steps are planned to be taken, and, if certain actions are not being taken, why not. Nor is it clear to the Commission that NERC has received a complete set of responses to its data request. Thus, it is important for the Commission to issue an order seeking information that would supplement NERC's action and provide more detailed information on which to assess the status of mitigation efforts.

If the OMB authorizes the Commission to collect this information, the Commission intends to issue the order and direct the submission of this information to NERC. Following Commission review of the information, the Commission will determine whether further action is necessary or appropriate. For example, the Commission may consider adopting an order that requires, pursuant to section 215, the expedited development of a reliability standard to ensure that mitigation measures are promptly and effectively implemented. However, Commission review of this information may also indicate that no further action is necessary or appropriate. Once complete, I plan to inform the Subcommittee of the results of the review and describe what further action, if any, may be taken to address the matter.

Your letter also asks whether the authority granted to the Commission under section 215 is adequate to address threats related to this or other cyber security vulnerabilities. As a general matter, there are three principal issues affecting the Commission's ability to address such specific threats adequately: (i) the timely and effective identification of a cyber vulnerability, (ii) the ability to adopt a mandatory reliability standard that mitigates that vulnerability on a timely basis, and (iii) the ability to maintain the confidentiality of information regarding that vulnerability during the standards development process, the Commission's approval process, and the compliance monitoring and enforcement process. As described in more detail below, section 215 has certain limitations that could impede timely responses to certain bulk power system vulnerabilities.

First, the Commission is not a national security or intelligence agency and therefore has limited ability to identify cyber vulnerabilities on a timely and effective basis. Nor are cyber threats limited to the bulk power system. For this reason, the Commission cooperates with the Department of Homeland Security, the Department of

Defense, and other governmental agencies to assess these vulnerabilities. These agencies are in a much better position than the Commission to assess the nature of cyber threats. The Commission has cooperated with these agencies with regard to the specific vulnerability referenced in your letter.

Second, cyber or other vulnerabilities associated with a terrorist threat can require swift remedial action to protect the Nation's bulk power system. The standards development process under section 215 requires reasonable opportunity for notice and public comment, openness and a balance of interests in the development of standards and, consequently, can be relatively slow. For example, it has taken years to develop new standards. Once standards are proposed, the Commission's approval process is governed by basic Administrative Procedure Act requirements. Within these statutory restrictions, the Commission has also approved a process for NERC's development of standards on an "urgent action" basis to accelerate this process. Since this urgent action process has not yet been applied under section 215, it is not clear whether it can be used effectively to address cyber or other similar threats within a very short time (e.g., within 30-90 days). Regardless, if the Commission determines that further action is warranted to address the identified cyber vulnerability, it will consider directing NERC to use its urgent action procedures to develop on an expedited basis a standard.

Third, this standards development process typically imposes few or no restrictions on dissemination of information related to the development of a new standard. Indeed, section 215 requires "openness" in the standards development process. However, in the case of a cyber or similar vulnerability, the public release of information related to the vulnerability could be very harmful. The Commission has some authority to limit the dissemination of such information, but the limits of that authority are not well defined. Additionally, the Commission does not have explicit authority, as do some agencies, to categorize information as "safeguard" information or some other category that allows information to be provided only on a "need to know" basis.

There are significant limitations in the use of the section 215 process to guard against cyber security threats to the bulk power system. However, I have not yet reached the conclusion that legislation is needed at this time.

Finally, you ask about the definitions of "critical assets" and "critical cyber assets" contained in the proposed CIP reliability standard CIP-002-1. Specifically, you ask whether the assets at issue in the ES-ISAC advisory would be considered "critical assets." In the CIP 002-1 standard currently pending at the Commission, the ERO proposed a process for identifying "critical assets" that would allow users, owners, and operators to determine what "critical assets" they own. Because the proposed process provides too much ambiguity and discretion to users, owners and operators, the Commission has proposed to direct that NERC modify it by requiring the ERO to provide more structured guidance about how to define a "critical asset" and by requiring a regional review process

to ensure consistency and rigor. Given the broad discretion and absence of specific guidance and review under the CIP standards proposed by the ERO, it is therefore unlikely that the users, owners or operators would consistently classify the assets identified in the ES-ISAC advisory as "critical." It is important to note that any improvements to the identification of "critical assets" directed by the Commission in the final rule will not be subject to mandatory compliance by the owners and operators of the vulnerable equipment until the CIP standards have been modified through NERC's standards development process and approved by the Commission.

If I or Commission staff can be of further assistance to the Subcommittee in this or any other matter, please do not hesitate to let me know.

Sincerely,

Joseph T. Kelliher
Chairman

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D. C. 20426

OFFICE OF THE GENERAL COUNSEL

OCT 23 2007

Nathan J. Frey
Desk Officer (FERC)
Office of Information and Regulatory Affairs
Office of Management and Budget
725 17th Street, N.W.
Washington, D.C. 20503

Dear Mr. Frey:

On behalf of the Federal Energy Regulatory Commission (Commission), we are requesting emergency approval, under 5 C.F.R. § 1320.13, for a one-time information collection request the Commission needs to undertake in order to evaluate the steps taken by the electric industry to mitigate a recently identified cyber vulnerability.

A recent experiment conducted for the Department of Homeland Security by the Idaho National Laboratory demonstrated that under certain conditions energy infrastructure could be intentionally damaged through cyber attack. In that experiment, researchers caused an electric generator to malfunction through an experimental cyber attack. This cyber vulnerability, which was recently broadcast on CNN, was the subject of an October 17, 2007 hearing before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House of Representatives, at which Commission staff testified. In addition, on October 17, 2007, the Chairman of the Commission received a letter from the full Committee on Homeland Security (attached), asking the Commission to immediately investigate the level of mitigation efforts by the electric industry.

In light of the seriousness of the cyber vulnerability and the need to assess whether the Commission needs to take steps to address the matter, the Commission intends to immediately issue a directive requiring all generator owners, generator operators, transmission owners, and transmission operators that are registered by the North American Electric Reliability Corporation (NERC) and located in the United States to provide to NERC certain information related to their mitigation measures in response to the threat to cyber security. The Commission will review this information, at NERC's offices, to determine whether any further measures need to be taken to improve cyber security in the electric industry. NERC is subject to the Commission's oversight under section 215 of the Federal Power Act, 16 U.S.C. § 824o.

Section 215 of the Federal Power Act, 16 U.S.C. § 824o, vests the Commission with authority over NERC and over the users, owners, and operators of the Nation's Bulk-Power System with respect to adopting and enforcing mandatory reliability standards, including cyber

security-related reliability standards. Section 307 of the Federal Power Act, 16 U.S.C. § 825f, authorizes the Commission to "investigate any facts, conditions, practices, or matters which it may find necessary or proper . . . to aid in . . . prescribing rules or regulations [under the Federal Power Act], or in obtaining information to serve as a basis for recommending further legislation." Section 39.2(d) of the Commission's regulations, 18 C.F.R. § 39.2(d), requires owners and operators to "provide the Commission . . . such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission."

The Commission is currently engaged in a rulemaking proceeding involving standards proposed by NERC for critical infrastructure protection related to cyber security.[1] However, these standards, even if they are approved by the Commission, are not proposed by NERC to be implemented until mid 2009 through 2010. Given the potential threat identified by the Idaho National Laboratory experiment, the Commission believes that it needs to act now to determine whether any further actions are necessary on an expedited or an emergency basis prior to the implementation of the standards addressed in the ongoing rulemaking process. The first step in this determination is that the Commission must be able to quickly discern the level of mitigation measures already taken within the electricity industry to date, and what mitigation is planned for the near future, as well as what actions will not be taken. The Commission's order will gather the necessary information and allow the Commission to review the mitigation plans of industry members, while both preserving confidentiality and minimizing any burden on the industry. While NERC did send a data request to its members late last week, that data request is limited in scope. It is limited to a request that industry members indicate if their mitigation plans are "complete," "in progress," or "not performing." This information is not sufficient for the Commission to discharge its duties under section 215 of the Federal Power Act because it does not provide information on what facilities are the subject of the mitigation plans, what steps to mitigate the cyber vulnerability are being taken, when those steps are planned to be taken, and, if certain actions are not being taken, why not.

The Commission's order, which it would plan to issue by Tuesday, November 13, 2007, would direct that the requested information be submitted to NERC by Tuesday, December 4, 2007, and that NERC make this information available for review by the Commission. NERC would be directed to secure the submittals, and treat the responses as nonpublic information available on a need-to-know basis to NERC personnel and to the Commission. This early deadline is necessary given the urgency of the cyber security issue and to comply with the House Committee's request. Thus, to accommodate this deadline, we request that OMB review the attached draft Proposed Information Collection and Request for Comments and make a determination that the Commission may issue the Proposed Information Collection statement by Friday, October 26, 2007. We anticipate publishing the Proposed Information Collection statement in the Federal Register on Friday, November 2, 2007, with comments due to the Commission and OMB by Wednesday, November 7, 2007. This schedule provides for comment by affected parties, while avoiding unnecessary delay.

---

[1] *See Mandatory Reliability Standards for Critical Infrastructure Protection*, Notice of Proposed Rulemaking, 72 Fed. Reg. 43,970 (Aug. 6, 2007), FERC Stats. & Regs. ¶ 32,630 (2007) (CIP NOPR).

The enclosed documents describe the proposed order, as well as provide further information on the urgency of this issue. We would be happy to discuss this further with you, if necessary, by telephone conference (Cynthia A. Marlette, (202) 502-6000; Joseph H. McClelland, (202) 502-8600) or by an in-person meeting.

Sincerely,

Cynthia A. Marlette

Cynthia A. Marlette
General Counsel

Joseph H. McClelland
Director, Office of Electric Reliability

Enclosures