BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

October 17, 2007

The Honorable Joseph T. Kelliher
Chairman
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Dear Chairman Kelliher:

The bulk-power system (BPS) of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people.[1] The effective functioning of this infrastructure is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. As such, there is an increasing risk that these systems – and the critical infrastructure that rely on the BPS – can be damaged or disrupted by both intentional and unintentional cyber incidents. Such incidents could potentially have a significant and potentially devastating impact on the economy, public health, and national security of the United States.[2]

In March 2007, the Idaho National Laboratory performed an experiment for the Department of Homeland Security (DHS) in which it successfully destroyed a generator while conducting an experimental cyber attack. According to news reports, the attack involved a controlled hack of a replicated control system commonly found throughout the BPS.[3] As Members of the House Committee on Homeland Security, we are concerned that malicious actors could use the same attack vector against larger generators and other

---

[1] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.

[2] For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion. See, e.g., "Mouse click could plunge city into darkness, experts say," (2007, Sept. 27), retrieved Sept. 28, 2007 from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[3] *Id.*

critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure of the United States.

Upon completion of the research, DHS and the Department of Energy (DOE) began working on mitigation strategies that would prevent the exploitation of this vulnerability. DHS requested that the North American Electric Reliability Corporation (NERC), acting through the Electric Sector Information Sharing and Analysis Center (ES-ISAC), issue a "required action" for entities in the electric sector to reduce the risks associated with the identified cyber vulnerability. On June 21, 2007, the ES-ISAC distributed an advisory describing the mitigation measures for electricity sector owners and operators. The measures are divided into time-sensitive categories:

1. Short-term measures need to be started immediately and completed within 60 days. These measures are basic cybersecurity practices and should already be in place by electricity sector owners and operators.

2. Mid-term measures should take 60 to 180 days to evaluate and implement. Electricity sector owners and operators will need to evaluate these measures and decide which measures need to be taken on their systems. They require longer lead times and engineering, assessment and evaluation.

3. Long-term measures are greater than 180 days. Electricity sector owners and operators will need to evaluate and consider implementing additional mitigation measures.

The advisory also contains mitigation efforts that must be implemented immediately if an exploit of the vulnerability is detected or if the vulnerability is disclosed in sufficient detail that an exploit is imminent. According to the advisory, notification of this condition will be supplied by the ES-ISAC or DHS.

Notably, a recent order issued by the Federal Energy Regulatory Commission (FERC) denied NERC's ability to issue "required actions" to electric sector owners and operators for incidents outside the scope of FERC-approved reliability standards. As the Electric Reliability Organization (ERO) certified under section 215 of the Federal Power Act (FPA), FERC determined NERC has authority only to require specific action in the context of violations or possible violations of Commission-approved reliability standards.[4] Because the Critical Infrastructure Protection (CIP) Reliability Standards for

[4] In a previous interpretation of NERC's Rules of Procedure, FERC allowed NERC to disseminate "operations and equipment alerts" that could require specific actions by bulk-power users, owners, and operators. NERC could disseminate this information in three ways: 1) advisory (purely informational); 2) recommendation; and 3) required action. FERC asserted that NERC should issue operations and equipment alerts only under NERC's remedial power. *See North American Reliability Corp.*, 119 FERC ¶ 61,248 (2007), p. 64. NERC sought clarification that it should use a remedial action directive because these directives must be based on a violation or possible violation of a Reliability Standard. *See Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 723, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672—A, FERC Stats. & Regs. ¶ 31,212 (2006).

cybersecurity are still under consideration by FERC, NERC cannot issue any directives to compel compliance; they are limited to disseminating "advisories" and "recommendations" to owners and operators.

This order has significant implications for the efforts to mitigate the cybersecurity vulnerabilities discovered by the Idaho National Laboratory. Though NERC's advisories may have persuasive power within the sector, there is no guarantee that BPS users, owners, and operators will implement these security practices. In arguments before the FERC, NERC maintained that "it is in the public interest for it to issue alerts to the industry requiring specific corrective actions where NERC obtains information showing the need for such corrective actions, even where a violation of a Reliability Standard is not involved."[5] We agree with this contention, and we are deeply concerned that the mitigations developed by DHS and DOE and recommended to the electric sector by the NERC have not been executed. The voluntary sector-partnership framework utilized by DHS for critical infrastructure protection is only valuable if it is able to confirm the degree to which its advisories are carried out by stakeholders within a relevant sector, sub-sector, or system.

The Committee recently learned that NERC sent two surveys to members of the electricity sector about the implementation of the advisory's mitigation measures. The first, sent two weeks after the issuance of the advisory, allegedly found that 15 percent of the sector implemented the advisory's mitigation measures; the second, sent four weeks after the issuance of the advisory, allegedly found that 100 percent of the sector implemented the advisory's mitigation measures.

We ask that you immediately commence an investigation to determine the level to which electric sector owners and operators have implemented these mitigation efforts. In determining the veracity of the NERC survey response, please also provide answers to the following questions:

1. When they obtained the ES-ISAC advisory in June, what percentage of owners and operators believed that these mitigation measures were recommendations? What percentage believed they were requirements? The NERC believes that it conveys "sufficient authority to persuade entities to comply" with alerts issued by the ES-ISAC.[6] Did the perception of obligation dictate the level of compliance?

2. If a cyber exploit of this vulnerability is imminent, how will the ES-ISAC or the Department of Homeland Security ensure the immediate implementation of mitigation efforts, given that the electric sector considers this an advisory document? Does the FERC possess regulatory authority to require immediate action? What structural challenges are preventing the complete mitigation of this vulnerability? Will Section 215

---

[5] *North American Electric Reliability Corporation* 120 FERC ¶ 61,239 (2007), *order on clarification* (emphasis added).
[6] *Id.*

of the Federal Power Act limit the ability of FERC and NERC to mount an immediate response to a similar incident in the future? Are any adjustments to the legal framework necessary?

3. The proposed CIP Reliability Standard 002-1 requires a responsible entity to identify its "critical assets" and "critical cyber assets" using a risk-based methodology, with the goal of ensuring that these assets are adequately protected from any potential cyber incident. NERC defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets." "Critical assets" are defined as "facilities, systems, and equipment that would affect the reliability or operability of the bulk-power system."[7] Under this definition, would the assets at issue in the ES-ISAC advisory be considered "critical assets"? If not, how can we ensure complete mitigation of this vulnerability? What does this say about the effectiveness of the proposed cybersecurity standards? Is a regulatory mandate necessary?

Thank you for your consideration of this request. If you have any questions, please contact Jacob Olcott, Subcommittee Director and Counsel, or Matt Washington, Subcommittee Director, Committee on Homeland Security at (202) 226-2616. We look forward to your timely reply.

Sincerely,

James R. Langevin

Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Michael T. McCaul

Honorable Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Sheila Jackson Lee

Honorable Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security and Infrastructure Protection

---

[7] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.