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

May 29, 2008

The Honorable John D. Dingell
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Dingell:

The Committee on Homeland Security has been conducting a review into the efforts of owners and operators of the bulk power system ("BPS") to secure their information networks. In testimony before this Committee, Joseph Kelliher, the Chairman of the Federal Energy Regulatory Commission ("the Commission"), stated that his agency is in need of additional legal authorities to adequately protect the BPS against cyber attack. We fully support the Chairman's request, and would like to work with you and your Committee to pass such legislation.

As you are aware, the 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 computer-based control systems that are used to monitor and manage sensitive processes and physical functions. Once largely proprietary, closed systems, these control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks."[2]

---

[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] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.

The risk to these systems is steadily increasing. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the BPS, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[3] Since the release of that study, numerous unintentional cyber incidents – the Davis-Besse power plant incident in 2003, the Northeast blackout in 2003, and the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted. Malicious actors also pose a significant risk to this infrastructure. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states, domestic criminals and hackers, and disgruntled employees working within an organization.[4]

Clearly, intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the United States. For a society that runs on power, the short term or long term disruption 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.[5] This figure does not consider the negative societal or health ramifications that such an event would have on the American people. With these issues in mind, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology initiated a review of the Federal government's effort and ability to ensure the security of the BPS from cyber attack.

In October 2007, the Subcommittee held a hearing on the cyber threat to control systems, focusing particularly on a vulnerability to the BPS discovered by engineers at the Idaho National Laboratory. The vulnerability – known as "Aurora" – could enable a targeted attack on infrastructure connected to the electric grid, potentially destroying these machines and resulting in catastrophic losses of power for long periods of time. After engineers demonstrated a successful test of the vulnerability, the Department of Homeland Security ("DHS"), the Nuclear Regulatory Commission ("NRC") and the Commission began leading an effort to reach out to the private sector to mitigate the vulnerability.

Under the framework of the Partnership for Critical Infrastructure Security,[6] DHS began its outreach efforts with the Electric and Nuclear sectors by identifying technical

---

[3] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.

[4] U.S. Government Accountability Office, Report to Congressional Requesters, *TVA Needs to Address Weaknesses in Control Systems and Networks* (April 2008), p. 8.

[5] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[6] The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

teams and establishing a set of subject matter experts to develop a mitigation strategy.[7] These two sectors began implementing the mitigations in varying degrees. On June 20, 2007, the Nuclear Sector issued a requirement for all members of their sector to implement short, medium, and long term mitigations for the vulnerability. On June 21, 2007, the Electric Sector (through the Electric Sector Information Sharing and Analysis Center, ES-ISAC) sent an advisory to its members with recommendations that they take similar action.

During the Subcommittee's hearing in October, it became evident that the Nuclear Sector was well on its way toward implementing the mitigations; however, the extent to which Electric Sector companies were following the recommendations of the advisory was not clear. The difference in each sector's implementation stemmed from the cybersecurity regulatory requirements. In October 2007, the Commission had not yet adopted the Critical Infrastructure Protection reliability standards proposed by the North American Electric Reliability Corporation ("NERC"), which addressed cybersecurity requirements for the Electric Sector. Therefore, while the NRC could issue specific requirements for its owners and operators, the Electric Sector was unable to make similar demands.[8] Members of the Committee expressed concern during the hearing that these mitigation measures were not being fully implemented in the Electric Sector.

These concerns were justified. Though NERC testified during the hearing that it sent a survey to industry members to determine compliance with the advisory and received a response from approximately 75 percent of the transmission grid that mitigations had been implemented or were in the process of being implemented,[9] the Committee later learned that the survey was not sent until October 19, 2007 – two days after the hearing.[10] Later, NERC staff suggested that they received information about the industry's mitigations efforts during a Critical Infrastructure Protection Committee meeting in St. Louis in September 2007. However, when the Committee asked participants about that meeting, none of the attendees were able to confirm that they discussed their mitigation efforts with NERC.

In light of these discrepancies, in mid-October 2007, the Subcommittee, on a bipartisan basis, requested that Chairman Kelliher investigate the level to which Electric Sector owners and operators implemented the mitigation efforts from the original

---

[7] The Department held briefings at the FOUO level rather than classifying the information to the Secret level. The Department's justification for this was the importance of having the private sector aware and involved with mitigation of the vulnerability.

[8] Several things have changed since the Subcommittee hearing. On January 17, 2008, the Commission approved eight mandatory critical infrastructure protection reliability standards to protect the bulk power system against potential disruptions from cyber security breaches. These standards were developed by NERC, the private sector organization designated by the Commission as the electric reliability organization (ERO). These standards are currently in effect, though the industry has until approximately 2010 before they have to demonstrate "auditable compliance" with the standards. See NERC Revised Implementation Plan for Cybersecurity Standards.

[9] U.S. Congress, House Committee on Homeland Security, Hearing on "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid," *testimony of David Whiteley,* 110th Cong., 1st sess., 17 Oct. 2007.

[10] Electric Sector ISAC (ESISAC) Advisory Follow-up Survey, Oct. 19, 2007.

advisory. Chairman Kelliher had expected to be able to draw upon results from NERC's October 19 industry survey; however, he determined that the survey lacked sufficient details of the mitigation efforts that would have provided the Commission with the certainty that the vulnerability had been addressed. For example, NERC's survey did not provide information about what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken – and, if certain actions were not being taken, why not. The Commission determined that it would have to undertake its own independent survey in order to obtain the information requested by this Committee.

We understand that the Commission is in the process of working with industry groups to informally gather information, on a voluntary basis, regarding the status of compliance with NERC's Aurora advisory. Initial observations suggest that while no company interviewed ignored the advisory, there was a broad range of compliance based on individual interpretations of the threat and the application of the recommended mitigation measures. In fact, all of the utilities interviewed requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, the Commission has determined that although progress has been made by every entity that it interviewed much work remains to be done.

Contemporaneous with its request for a Commission-led investigation, the Subcommittee also requested that the Commission assess its ability to respond to an imminent cyber attack under the current legal authorities contained in Section 215 of the Federal Power Act ("FPA"). We were concerned that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the promulgated standards, but also the authority to issue orders to owners and operators in the event of an imminent exploitation of a BPS asset.[11] In testimony before the Subcommittee on May 21, 2008, Chairman Kelliher concluded that additional authorities are necessary to adequately protect the BPS against cyber attack. The Chairman noted that while Section 215 may adequately protect the BPS against most reliability threats, the cybersecurity threat is different:

> [Cybersecurity] is a national security threat that may be posed by foreign nations, or others intent on undermining the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Given the national security dimension to the cyber security threat, there may be a

[11] This Committee has argued that the NERC reliability standards are inadequate for protecting critical national infrastructure. For instance, telecommunications equipment is excluded from the standard's definition "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations. Ironically, some of these assets that could be exploited in an attack using the Aurora vulnerability are not considered "critical cyber assets." This means that if the Aurora vulnerability was discovered again tomorrow, NERC could not issue a "required action" to owners and operators under its jurisdiction because the "assets" affected by the Aurora vulnerability are not currently covered by CIP standards.

need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action.[12]

We fully agree with the Chairman's conclusion. In the interest of national security, a statutory mechanism is necessary to protect the grid against cyber security threats. We believe that the FPA should be amended to grant the Commission emergency authority to order temporary interim cybersecurity or other emergency standards when necessary to protect against a national security threat to the reliability of the BPS. These standards should become enforceable upon a finding by a national security or intelligence agency that there is a national security threat to the BPS. This authority should also address circumstances under which information contained in the order could be kept confidential, such as when the information, if revealed to the public, could reasonably be expected to have a significant adverse effect on the safety of the public or common defense or national security.

We look forward to working with you and your Committee to pass this critical legislation. If you have any questions, please contact Jacob Olcott, Subcommittee Director and Counsel, or Rosaline Cohen, Chief Counsel, Committee on Homeland Security, at (202) 226-2616.

Sincerely,

Bennie G. Thompson
Chairman
Committee on Homeland Security

James R. Langevin
Chairman
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Committee on Homeland Security

[12] U.S. Congress, House Committee on Homeland Security, Hearing on "Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid," *testimony of Joseph Kelliher*, 110th Cong., 2nd sess., 21 May 2008. Chairman Kelliher noted that "cyber vulnerabilities can require swift remedial action to protect the Nation's bulk power system," and that the standards development process can be "relatively slow." Furthermore, even though the Commission has an "Urgent Action" process, this can take one to three months to implement.