Statement of James R. Langevin
Chairman, Emerging Threats, Cybersecurity,
Science and Technology Subcommittee
U.S. House of Representatives Committee on Homeland Security

Hearing before the House Committee on Energy and Commerce
Subcommittee on Energy and Air Quality
September 11, 2008

I. Introduction and Overview

Good morning. I'd like to begin by thanking Chairman Boucher for his invitation to allow me to testify on this critical issue of national security. I very much appreciate the Chairman's interest in the subject of cybersecurity as it relates to the electric grid, and I commend him, the full Committee, and the staff for their efforts in this area. I would also like to thank Chairman Thompson of the Homeland Security Committee for his proactive leadership on cybersecurity and other issues of national security.

I serve as Chairman of the Emerging Threats, Cybersecurity, Science and Technology Subcommittee for the Homeland Security Committee, where I have held eight hearings and conducted dozens of investigations on cybersecurity issues during the 110th Congress. During this time, the Committee on Homeland Security conducted a review into the efforts of owners and operators of the bulk power system ("BPS") to secure their information networks. I want to clearly state that I believe America is disturbingly vulnerable to a cyber attack against the electric grid that could cause significant consequences to our nation's critical infrastructure. Virtually every expert that I've discussed these matters with – across government and throughout the private sector – shares this assessment. Though I cannot provide classified details at this hearing, I hope that the following sections will support this assertion.

In testimony before the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology on May 21, 2008, Chairman Joseph Kelliher 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. I fully support the Chairman's request for these authorities. However, I am concerned that the current legislation does not cover assets that are outside the scope of the Federal Power Act definition of BPS, which, if left unprotected, will keep our nation vulnerable. I respectfully submit the following comments for the Committee's consideration.

II. Background: Threats and Vulnerabilities to the BPS

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 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. 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]

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 – from the Davis-Besse power plant incident in 2003, to the Northeast

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

blackout, to 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]

There are numerous public examples of threats and vulnerabilities that have had a negative and dangerous impact on electric systems. The potential consequences of an attack on control systems vary widely from the introduction of raw sewage into potable water systems[5] to the catastrophic failure of critical electrical generators due to the change of a single line of code in a critical system.[6] For example:

- Computers at an inactive nuclear power plant in Ohio were infected by the Slammer worm in January 2003.[7]
- Multiple criminal extortion schemes have exploited the use of control systems for economic gain.[8]
- There is evidence that al Qaeda is interested in the vulnerabilities of the U.S. public and private utilities.
- The discovery in Afghanistan of a computer containing structural analysis programs for dams, combined with an increase in Web traffic relating to SCADA systems, prompted the National Infrastructure Protection Center ("NIPC") to issue a warning information bulletin.[9]
- Nation state adversaries have suggested that attacking our domestic critical infrastructure will be part of their war plans in an engagement with the United States. In a book endorsed by top Chinese People's Liberation Army leadership called "Unrestricted Warfare," two colonels describe using network attacks "to

[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] U.S. Government Accountability Office, Report to Congressional Requesters, *Challenges and Efforts to Secure Control Systems* (2004) p. 17..
[6] Briefing by NCSD, INL to the Homeland Security Committee, March 15, 2007.
[7] Congressional Research Service "Critical Infrastructure: Control Systems and the Terrorist Threat," RL31534, p. 17.
[8] Infoworld, "Government cybersecurity gets an 'F,'" Sep. 11, 2006, available at http://www.infoworld.com/article/06/09/11/37NMmain_1.html.
[9] CRS Report RL31534, p. 7.

> disrupt the civilian electricity network, traffic dispatching network, financial transaction network, and telephone communications networks," causing social panic and undermining political leadership.

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 discontinuity of electricity to chemical plants, banks, refineries, hospitals, and water systems 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.[10] This figure does not consider the negative societal or health ramifications that such an event would have on the American people.

An intentional or unintentional attack would also severely impact the ability of our war fighting capability. The Defense Science Board recently recognized the threat to critical Department of Defense ("DOD") military facilities that rely on the BPS. In a report titled "More Fight – Less Fuel" issued in February 2008, the Board concluded that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid and other critical national infrastructure."[11] The Board stated the grid "is highly vulnerable to prolonged outage from a variety of threats. This places critical mission assets at unacceptably high risk of extended disruption."[12] Furthermore, in the event of an attack on the BPS, the Board noted that the U.S. military cannot rely on on-site backup power generation:

> Although 99 percent of the electricity at U.S. military installations is from the commercial grid, backup power at installations is based on diesel generator sets with limited on-site fuel storage and not prioritized to critical tasks. As the reliability of the national grid has declined, the

[10] (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.
[11] Report of the Defense Science Board Task Force on DOD Energy Strategy, *More Fight – Less Fuel*, February 2008, available at http://www.acq.osd.mil/dsb/reports/2008-02-ESTF.pdf.
[12] Id., p. 53.

> adequacy of backup power has become an issue. For both war fighting-related activity and the new Homeland defense mission, backup power is inadequate in terms of size, duration and reliability.[13]

The Board concluded that the DOD's approach to providing power to installations is based on assumptions that commercial power is highly reliable, subject to infrequent and short term outages, and backup can meet demands. Unfortunately, DOD's assumptions about commercial power and other critical infrastructure reliability are no longer valid and DOD must take a more rigorous risk-based approach to assuring adequate power to its critical missions. In the interest of national and homeland security, we must ensure effective and reliable energy flows to America's critical infrastructure facilities.

III. Homeland Security Committee Oversight: Aurora Investigation

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,[14] DHS began its outreach efforts with the Electric and Nuclear sectors, which each identified a technical team and a set of subject matter experts to develop a mitigation

[13] Id.
[14] 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.

strategy.[15] 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.[16] 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,[17] the

[15] 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.

[16] 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.

[17] 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.

Committee later learned that the survey was not sent until October 19, 2007 – two days after the hearing.[18] Later, NERC staff suggested that they received information about the industry's mitigation 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 extent to which Electric Sector owners and operators implemented the mitigation efforts from the original Aurora 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 the Homeland Security Committee.

The Commission is currently 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.

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

I was deeply disturbed that a thoroughly tested vulnerability which could cause catastrophic damage to the BPS was not being mitigated by the private sector. I began searching for other means by which we – the U.S. Congress – could ensure that the BPS (and the American populace that relies on its effective function) is being protected against these vulnerabilities. Therefore, contemporaneous with its request for a Commission-led investigation, my 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"). I was concerned that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the promulgated standards,[19] but also the authority to issue orders to owners and operators in the event of an imminent exploitation of a BPS asset.

In testimony before the Subcommittee on May 21, 2008, Chairman Kelliher agreed with my preliminary assessment, and 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

[19] The Homeland Security Committee has also 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.[20]

IV. Comments on the Draft Legislation

I fully support the Chairman's conclusion. In the interest of national security, a statutory mechanism is necessary to protect the grid against cybersecurity threats. I 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. I have several comments on the draft legislation.

First, I believe that emergency standards should become enforceable upon a finding by a national security or intelligence agency in consultation or coordination with FERC that there is a national security threat to the BPS. I fear that the Presidential/Secretarial determinations, as currently provided for in the draft legislation, could create unnecessary delays in the protection of the BPS. An event in cyberspace may happen in seconds, but determining to authorize authorities for a response could take hours or days – time that we simply cannot afford to waste.

Second, I believe that the President or the Department of Energy (or intelligence authorities, as suggested above) should be authorized to direct FERC action if either (1) a malicious act is likely to occur or (2) there is a substantial possibility of disruption to the grid due to such an act. Thus, I would recommend that the definition read "Cybersecurity threat means that there is credible information or evidence of (1) the likelihood of a

[20] 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.

malicious act that could disrupt the operation of those programmable electronic devices and communications networks…that are essential to the reliable operation of the bulk power system; or (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act."

Finally, the scope the bill is limited to facilities that comprise the BPS as defined in section 215 of the FPA. I feel compelled to discuss what I believe is a conceptual error in the FPA's definition of the BPS. The BPS is defined as the generation plants, the high voltage transmission system, and associated equipment, and does not normally include the distribution substations and lower voltage networks that distribute electricity to customers in a particular city or region. Alaska and Hawaii are specifically excluded from reliability regulations. In practice, many major cities and population centers are also excluded. This limitation leaves our nation vulnerable.

In January 2008, FERC approved the reliability standards developed by NERC to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. By definition and design, the BPS CIP Standards do not recognize the importance of continuity of electric power to chemical plants, banks, refineries, hospitals, water systems, and military installations, in and of themselves. Where they are located or their importance to society is not a factor in the determination of what parts of the greater U.S. electric system should be protected. This means that <u>any</u> Critical Infrastructure Protection ("CIP") Standards – including those recently approved by FERC – will focus on reliability of the BPS exclusively, and not on public health and safety or even economic stability from a "homeland security" perspective.

Before the terrorist attacks against our country on September 11, 2001, a single-minded focus on BPS reliability against serendipitous hazards and accidents may have been appropriate; but with the specter of terrorist or nation-state-directed force against the

U.S. public at large, preoccupation with the BPS as a whole falls short of the mark. For example, the reliable operability of a small substation powering a major oil or gas pipeline in a remote region is not important to the stability of the BPS grid, but an extended failure of that asset could very well have profound adverse consequences for the stability, and even the viability, of the U.S. economy or national security. I believe those small substations should be covered under Federal regulation.[21]

If the correct objective of the national electric power system is to generate, transmit, and reliably deliver electricity all the way out to the eventual end user – the public – then there are more links in this mission-chain than just the BPS, and the CIP Standards fall short of the mark. To enhance the national security, I believe this is an issue that the Committee on Energy and Commerce must re-examine.

For purposes of this legislation, I would ask the Members to consider an amendment that would allow FERC to direct measures or actions aimed at protecting Alaska, Hawaii, and the territories from reliability threats, as well as distribution facilities. This would cover most or all of the grid facilities in large cities such as New York and Washington, D.C., and the nation's critical military installations that are connected to the BPS. In passing this amended legislation, this Committee would truly be protecting the national electric system.

V. Conclusion

Thank you for allowing me the opportunity to speak to you today on such an important matter facing our nation. The Homeland Security Committee will continue to remain diligent in investigating cybersecurity issues across the Federal government and

[21] Note that the BPS Transmission grid in the area hardest hit by Hurricane Katrina was restored within six days following the storm, but that did not help get municipal water department pumps back up and running because the Distribution systems were still off-line. The public in many hurricane-affected areas did not have running water for a considerable period of time. A hacker incursion resulting in disability of a Distribution control system(s), and/or key assets thereby managed, can be a BPS-independent event that still results in, by example, the pumps of an urban water system being disabled with the same adverse end result for the public. In this specific example, reliable delivery of power to the water infrastructure is also a health and safety issue, not just an inconvenience for the public.

throughout the national critical infrastructure. I look forward to working with the Committee on Energy and Commerce on these and other national security issues in the future.