Statement of
Steven T. Naumann
Vice President, Wholesale Market Development, Exelon Corporation
On Behalf of the Edison Electric Institute and the Electric Power Supply Association

Before the
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Committee on Homeland Security
United States House of Representatives

July 21, 2009

Mr. Chairman and Members of the Subcommittee:

My name is Steve Naumann, and I am Vice President for Wholesale Market Development for Exelon Corporation. I also serve as Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC). I appreciate your invitation to appear today and the opportunity to testify about protecting the electric grid from cyber security threats.

Exelon is a holding company headquartered in Chicago. Our retail utilities, ComEd in Chicago and PECO in Philadelphia, serve 5.4 million customers, or about 12 million people – more than any other electric utility company. Our generation subsidiary, Exelon Generation, owns or controls approximately 30,000 MW of generating facilities, including fossil, hydro, nuclear and renewable facilities. Our nuclear fleet consists of 17 reactors; it is the largest in the nation and the third largest in the world.

I am appearing today on behalf of the Edison Electric Institute (EEI) and the Electric Power Supply Association (EPSA). Exelon is a member of both. EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members worldwide. EEI's U.S. members serve 95% of the ultimate customers in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. EPSA is the national trade association

representing competitive power suppliers, including generators and marketers. EPSA members own 40 percent of the installed generating capacity in the United States, providing reliable and competitively priced electricity from environmentally responsible facilities.

My testimony focuses on the nature of cyber security threats to the bulk power electric system and the efforts of electric utilities to respond to those threats. At the Subcommittee's request, I also will share suggestions and observations regarding the relationship between government and the private sector in our efforts to secure the electric grid from cyber attacks.

I want to assure the Subcommittee that as owners, operators, and users of the bulk power system, electric utilities take cyber security very seriously. We are actively engaged in addressing cyber security threats as they arise and in employing specific strategies that make every reasonable effort to protect our cyber infrastructure and mitigate the risks of cyber threats. As the industry relies increasingly on electronic and computerized devices and connections, and the nature of cyber threats continually evolves and becomes more complex, cyber security will remain a constant challenge for the industry. But we believe we are up to the task, building on our industry's historical and deep-rooted commitment to maintaining system reliability.

Industry Standards, Emergency Authority and Legislative Proposals

The industry believes it is appropriate for Congress to consider legislation providing the Federal Energy Regulatory Commission (FERC) new emergency authority to address imminent cyber security threats. I want to emphasize, however, that current law already provides the means to address many cyber security issues in the electric industry. Section 215 of the Federal Power Act (FPA), which was enacted by Congress as part of the Energy Policy Act of 2005, provides for mandatory and enforceable electric reliability rules, specifically including rules to address cyber security with FERC oversight.

The basic construct of the relationship between FERC and NERC, which FERC certified as the Electric Reliability Organization (ERO) under FPA Section 215, in developing and enforcing reliability rules is sound. In summary, NERC, using a well-defined stakeholder process that leverages the vast technical expertise of the owners, users, and operators of the North American electric grid (including those in Canada with whom we are interconnected) develops reliability standards, which are then submitted to FERC for review and approval. Once approved by FERC, these standards are legally binding and enforceable in the United States. NERC also submits these standards to regulatory authorities in Canada.

I suggest the question on which the Subcommittee should focus is, "What additional authority should be provided to FERC in order to promote clarity and focus in response to imminent cyber security threat situations?" Legislation in this area should complement, not supplant, the mandatory reliability regime already established under FPA Section 215, and any new FERC authority should be appropriately narrow and focused only on unique problems that cannot be addressed under Section 215. The FPA Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation.

Any cyber security legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. Consultation is critical to improving cyber security.

Obviously, the scope of the damages that could result from a cyber security threat depends on the details of any particular incident. A carefully planned cyber attack could potentially have serious consequences. In considering the scope of damages that any particular cyber security threat might inflict, utilities must also consider the potential consequences caused by any measures taken to prevent against cyber attack. Certain

measures that might prevent a particular type of cyber attack could themselves have adverse impacts to safe and reliable utility operations and service to electricity customers. Examples might include slower responses during emergency operations, longer times for restoration of outages and disruption of business operations dependent on Internet access. That is why each situation requires careful consultation with utilities to ensure that a measure aimed at protecting the grid from a malicious cyber attack does not instead cause other unintended and harmful consequences.

Furthermore, every utility operates different equipment in different environments, making it difficult to offer generalizations about the impacts to the bulk power system or costs and time required to mitigate any particular threat or vulnerability. This complexity underscores the importance of consultation with owners, users, and operators to ensure that any mitigation that may be required appropriately considers these factors to ensure an efficient and effective outcome.

For the foregoing reasons, any new legislation giving FERC additional statutory authority should be limited to true emergency situations involving imminent cyber security threats where there is a significant declared national security or public welfare concern. In such an emergency, it is imperative that the government provide appropriate entities clear direction about actions to be taken, and assurance that those actions will not have significant adverse consequences to utility operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

Because of its extraordinary nature and potentially broad impacts on the electric system, any additional federal emergency authority in this area should be used judiciously. Legislation granting such authority should be narrowly crafted and limited to address circumstances where the President or his senior intelligence advisors determine there is an imminent threat to national security or public welfare.

Public-Private Partnerships: Collaboration and Communication

The following comments address the specific issues raised by the Subcommittee' invitation to testify regarding how government and the private sector share information before, during, and after cyber security attacks.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and electric utilities in ensuring the cyber security of the nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for ongoing consultation and sharing of information between government agencies and utilities.

Information about cyber security vulnerabilities and attempts to exploit those vulnerabilities is shared with electric industry owners, users, and operators through a number of channels every day. Federal agencies that communicate this information to the private sector, such as the United States Computer Emergency Readiness Team (US-CERT), as well as cyber security hardware and software vendors, classify vulnerabilities in terms of the generalized risk to systems. Factors such as the seriousness of consequences of a successful attack, the sophistication required to conduct the attack, and how widely used the potentially affected assets are within an industry are used to rank vulnerabilities as "high", "medium", or "low" risk.

Fundamentally, however, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of inherent limitations on its access to intelligence information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers,

and we understand how our complex systems are designed and operate. Owners, users, and operators of the bulk power system are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation. Greater cooperation, coordination and intelligence sharing between government and the private sector should be encouraged, consistent with the public-private partnership model endorsed by the President's 60-day cyber security review.

Exelon, for example, is addressing the risks we know about through a "defense-in-depth" strategy while appropriately balancing considerations of potential consequences. This defense-in-depth strategy includes preventive monitoring and detective measures to ensure the security of our systems. We perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform us about whether our preventive strategies are working so that we can enhance our protection as technologies and capabilities evolve. These penetration tests, which allow us to practice and enhance our monitoring capabilities, also yield lessons learned that are unique to our system. Because no two utility companies have identical network, hardware or logistical configurations, no single entity will know our system's strengths or weaknesses quite like we do.

NERC, which functions as the Electric Sector Information Sharing and Analysis Center (ISAC), disseminates alerts to provide information to the electric industry. With the input of its members, NERC has revised its procedures significantly over the past two years to improve the ability to quickly and securely provide this critical information to industry. This should ensure that when new vulnerabilities are uncovered, that users, owners and operators will receive the needed information in a timely manner to take corrective action. Thus, we believe that the ISAC is providing timely and relevant analysis and alerts to the industry. Many of us have been frustrated with NERC's historically slow information sharing process. I am pleased to note they have improved and we are getting information in a much more timely manner, though like anything else, there is always room for more improvement.

Smart Grid

As grid technologies continue to evolve and become "smarter," they inevitably will include greater use of digital controls. Congress recognized the potential cyber security vulnerabilities, as well as benefits, that could result from greater digitization of the grid when it directed DOE to study these issues in Section 1309 of the Energy Independence and Security Act of 2007. Manufacturers of critical grid equipment and systems must fulfill their security responsibilities by adopting good security practices in their organizations, building security into their products, and establishing effective programs so that, as new vulnerabilities are discovered, they can inform customers and provide technical assistance with mitigation. As new smart grid technologies are developed, it is imperative for the industry to work closely with vendors and manufacturers to ensure they understand that cyber security is essential so that protections are incorporated into devices as much as possible.

It is equally critical that cyber security solutions be incorporated into the architecture being developed for smart grid solutions, so that the great benefits new smart grid technologies will provide are implemented in a secure fashion. With smart grid solutions in the early stages of development, opportunities exist to ensure this vision is fulfilled. EEI supports the process currently underway at the National Institute of Standards and Technology (NIST) to develop a framework of standards that will become the foundation of a secure, interoperable smart grid. It is imperative that NIST proceed boldly and expeditiously to establish standards applicable to all.

EEI is encouraging the development of a security certification program, through which smart grid components and systems could undergo independent testing and receive a certification that security tests had been passed. Such a program would help utilities differentiate among different vendor solutions to select those providing appropriate cyber security.

Finally, I would like to provide the Subcommittee information on advanced metering implementation by Exelon's operating utilities. ComEd will be installing Advanced Metering Infrastructure under an Illinois Commerce Commission approved pilot program. PECO is installing smart meters in accordance with Pennsylvania law that requires distribution companies to deploy smart meters for all customers over 15 years. Cyber security has been a cornerstone of Exelon's Smart Grid/Advanced Meter Strategy from its inception in early 2008. Exelon understands and recognizes the potential risks associated with the deployment of such technologies throughout its service territories and treats Cyber Security with the utmost importance. To ensure security of these installations, Exelon is following internally developed security requirements and documenting them in requests for proposals to vendors for the supply of Smart Grid/Advanced Meter solutions. This includes the requirement to enumerate vendor security capabilities that ensures confidentiality, integrity, and availability. Exelon maintains a vulnerability management program which requires a documented penetration test to demonstrate that controls are implemented as designed. Third party vendor audits are also performed to ensure vendor design & manufacturing controls are adequate. From an industry community and vendor perspective, Exelon is an active participant in the NIST Smart Grid Roadmap and Security Strategy development initiative and actively participates in other industry groups. ComEd and PECO will seek recovery of 100% of their costs of metering infrastructure in rate cases – as they do for all other infrastructure – except to the extent ComEd and PECO receive stimulus funding for advance meters. ComEd and PECO both plan to apply to DOE for Smart Grid Investment Grant (SGIG) funds to support their overall smart grid deployment efforts. Greater security is one of the benefits of the smart grid that DOE has articulated. Pursuant to this, SGIG applications are required to detail the cyber security implications of any project seeking funding. Cyber security has been a key consideration in the development of ComEd and PECO's smart grid plans and will be further detailed in their respective grant applications.

Conclusion

While many cyber security issues are already being addressed under current law, we believe it is appropriate to provide FERC with explicit statutory authority to address cyber security in a situation deemed sufficiently serious to require a Presidential declaration of emergency. In such a situation, the legislation should clarify the respective roles, responsibilities, and procedures of the federal government and the industry, including those for handling confidential information, to facilitate an expeditious response.

Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation for developing reliability standards. Any new authority should also be narrowly tailored to deal with real emergencies; overly broad authority would undermine the collaborative framework that is needed to further enhance security.

Promoting clearly defined roles and responsibilities, as well as ongoing consultation and sharing of information between government and the private sector, is the best approach to improving cyber security. Each cyber security situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the bulk power system.

Exelon and other electric utilities remain fully committed to working with the government and industry partners to increase cyber security.

I appreciate the opportunity to appear today and would be happy to answer any questions.