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
Homeland Security and Governmental Affairs Committee
United States Senate

June 15, 2010

Mr. Chairman and Members of the Committee:

My name is Steve Naumann, and I am Vice President for Wholesale Market Development for Exelon Corporation. I have participated on committees, task forces and working groups of the North American Electric Reliability Corporation (NERC) and recently completed serving as Chairman of NERC's Member Representatives Committee. I appreciate your invitation to appear today to discuss securing the North American electric grid against cyber threats, and the opportunity to testify about the Protecting Cyberspace as a National Asset Act of 2010. At the outset I would like to thank Chairman Lieberman, Ranking Member Collins and Senator Carper for the thoughtful approach taken in the bill and for your leadership on this issue.

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.

Both EEI and EPSA also are part of a broader coalition of electric power stakeholders. While I am not officially testifying on its behalf, this coalition includes several major trade associations representing the full scope of electric generation, transmission and distribution in the United States, as well as regulators, Canadian interests and large industrial consumers. Rarely do these groups find consensus on public policy issues, but in the case of securing the electric grid, there is near unanimous support for a regime that leverages the strength of both public and private sectors to improve cyber security.

My testimony focuses on the value of this cooperative relationship, the unique nature of threats to the power grid, and the ongoing efforts of the Nation's electric sector to respond to those threats. I also will share observations related to the Committee's bill, particularly appreciation for its adherence to three principles the industry believes are integral to successful cyber security policy. These include:

- Leveraging public and private sector expertise, while including robust information sharing between government and the private sector, as well as among other stakeholders;
- Limiting the scope of any new authority to emergencies that will affect truly critical infrastructure; and,
- Addressing threats and vulnerabilities in a comprehensive way, including a multi-sector approach that uses a government-wide coordinator to deal with the various critical infrastructure sectors.

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.

Fundamentally, however, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of limitations on its access to classified information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. Thus the government is able to detect threats, evaluate the likelihood of a malicious attack and the risk of an attack and utilize its expertise in law enforcement. 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 electric grid are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation, including ensuring against

unintended consequences of remedial actions. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more secure system for our customers.

Thus, the industry appreciates that greater cooperation, coordination and intelligence sharing between government and the private sector is built into the Committee's legislation that we are discussing today.

I would add that simply creating mechanisms for information sharing is only part of the solution. Those lines of communication must be developed at the highest levels of both government and industry, and then drilled on a regular basis to ensure that, in times of crisis, those with relevant information and operational expertise can communicate seamlessly, quickly and when needed, securely.

Another important component is your legislation's narrow scope; it focuses appropriately on the need to protect truly critical assets. There is a security axiom that states: if you try to protect everything, you protect nothing. Put another way, the risk-based prioritization reflected in the proposed bill ensures both government and private sector resources are allocated wisely.

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 detection 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.

Reinforcing the need for a private sector role in threat mitigation, 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 power companies have identical network, hardware or logistical configurations, no single entity will know our system's strengths or weaknesses quite like we do. The legislation recognizes these different characteristics of our systems by authorizing the Director of the National Center for Cybersecurity and Communications to approve alternative measures submitted by owners or operators to protect critical infrastructure against the threat.

The industry believes new emergency authority to address imminent cyber security threats is appropriate. 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 giving the Federal Energy Regulatory Commission (FERC) oversight authority over cyber security rules.

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 applaud the Committee for addressing what additional authority is needed 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 government 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.

The importance of government-industry cooperation and consultation cannot be overstated. 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.

Furthermore, every power company operates different equipment in different regulatory 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. Costs in particular are an important part of the equation, as the uncertainty associated with federally directed cyber security orders, where the scope of an attack and the required remedies are an unknown and thus cannot be planned for, creates an outstanding question related to economic feasibility and capability. This complexity underscores the importance of consultation with owners, users, and operators, as well as state and federal regulators, and where time permits, prior consultation, 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 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 power operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

Finally, I would like to extend thanks for your vision to address cyber security using a comprehensive, multi-sector approach. While EEI, EPSA and Exelon's interests lie with protecting the electric grid, the interconnected nature of critical infrastructure prevents us from claiming victory unless a comprehensive approach is taken. Electric utilities, for example, rely on telecommunications systems to operate the grid, pipelines to fuel our generation, and wholesale markets to sell our product. Should any of these critical sectors be compromised, the electric grid would be impacted as well. Likewise, each of these sectors relies on the electric grid for the power they need to operate. Your bill recognizes this truth, as did the President's "60-Day Cyber Review" completed last year. I would urge the Congress to follow your leadership and approach this issue in a holistic manner.

Conclusion

While many cyber security issues already are being addressed under current law, we believe it is appropriate for the government 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 critical infrastructure industries, 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 also should 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 electric grid.

Exelon and other electric power stakeholders remain fully committed to working with the government and industry partners to increase cyber security and appreciate the efforts of this Committee to advance legislation that would create such a framework.

Thank you again for the opportunity to appear today; I would be happy to answer any questions.