Statement of
Steven T. Naumann
Vice President, Wholesale Market Development
Exelon Corporation

On Behalf of
Edison Electric Institute
and
Electric Power Supply Association

Before the
Subcommittee on Energy and Air Quality
Committee on Energy and Commerce
U.S. House of Representatives

September 11, 2008

Executive Summary
Statement of Steven T. Naumann
Exelon Corporation
On Behalf of
Edison Electric Institute and Electric Power Supply Association

Electric utilities take cyber security very seriously and are actively engaged in identifying and employing strategies to protect our cyber infrastructure and mitigate the risks of cyber threats.

While many cyber security issues are already being addressed under current law, it is appropriate to provide FERC with explicit statutory authority to address cyber security in certain emergency situations. 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 legislation should clarify the respective roles, responsibilities, and procedures of the federal government and the industry; be narrowly tailored to deal with real emergencies; and promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures.

Electric utilities routinely monitor for—and detect—electronic probing of their systems from a variety of sources, confirming the likelihood of real cyber security threats. However, utilities and other private sector entities are at a disadvantage in assessing the degree and urgency of possible or perceived cyber threats because of their limited access to intelligence information possessed only by the government. Electric utilities *are* in a unique position to understand the consequences of a potential malicious act on their systems as well as proposed preventive and mitigation actions. Therefore, the optimal approach to ensuring the cyber security of the bulk power system utilizes the respective strengths of both government intelligence specialists and electric utilities, and provides for ongoing consultation and sharing of information between government agencies and utilities.

The scope of the damages that could result from a cyber security threat depends on the details of any particular incident. Because utility operations vary greatly, it is difficult to generalize about the impacts of a particular threat, or about costs and time required to mitigate a threat or vulnerability. A carefully planned cyber attack could potentially have serious consequences. In mitigating a particular cyber security vulnerability, electric utilities must also consider the potential consequences caused by any mitigation measures on safe and reliable utility operations.

As the electric utility industry relies increasingly on digital information and controls, it must work closely with vendors and manufacturers to ensure that cyber security protections are incorporated into devices as much as possible. It is equally critical that the architecture underpinning cyber security solutions for the grid and the architecture being developed for smart grid solutions are synchronized and compatible so that the smart grid solutions and the great benefits they will provide will be implemented in a secure fashion.

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 Vice Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC). I am accompanied today by Dan Hill, Exelon's Senior Vice President and Chief Information Officer, who has day-to-day responsibility for cyber security issues in our company. 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 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), of which Exelon is a member. 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.

I am also testifying today on behalf of the Electric Power Supply Association (EPSA), of which Exelon is also a member. EPSA is the national trade association representing competitive power suppliers, including generators and marketers.

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. I want to reassure the Subcommittee that electric utilities and other owners, operators, and users of the bulk power system 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.

Legislation Generally

I agree with other witnesses that it is appropriate for Congress to consider legislation providing the Federal Energy Regulatory Commission (FERC) new authority to address emergency 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, which this Subcommittee helped develop and 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, under FERC oversight.

The basic construct of the relationship between FERC and NERC 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, 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.

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 emergency situations?" Legislation in this area should complement, not supplant, the mandatory reliability regime already established under 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 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. To the extent practicable, the construct provided by existing law should be replicated for imminent cyber security threats.

Specific Issues Related to Risks and Mitigation

The following comments address the specific issues raised by the Subcommittee in its invitation to testify:

- **The degree and urgency of the perceived risks to the bulk power system and those it serves and the evidence that such risks are real based on experience (limited to unclassified information).**

Because electric utilities and other companies routinely monitor for—and through such monitoring detect—electronic probing of our systems from a variety of sources, we must assume there is a real cyber security threat that all private sector entities face, including utilities. There is other generally available evidence that cyber security threats are real in the form of publicized events regarding exploitation of cyber security vulnerabilities, but it is important to note that to my knowledge no documented exploitation of electric utility systems affecting the North American bulk power system has occurred to date.

Fundamentally, however, the private sector is at a disadvantage in assessing the degree and urgency of possible or perceived cyber threats because of our limited 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 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 an exploitation. 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.

- **The extent to which the utility industry and other key participants in grid operations are or are not already prepared or currently undertaking protective measures.**

Exelon, like other utilities, takes cyber security extremely seriously. We are 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. For example, 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. Penetration testing also allows us to practice and enhance our monitoring capabilities.

Exelon responded to the "Aurora" vulnerability after learning about it through our nuclear business unit and then through an advisory that was sent to the electric industry by NERC in the summer of 2007. "Aurora" is a government laboratory's code name for a vulnerability that could allow an unauthorized person who gained remote access to certain electronic devices to cause damage to other pieces of equipment. We have taken the recommended actions to mitigate the vulnerability. While I do not have firsthand knowledge of what other utilities have done, based on my knowledge of the industry and conversations with my peers at other utilities, I believe other similarly situated utilities have also taken the risk seriously and have responded in an appropriate fashion.

- **The scope of damages that could be inflicted if adequate protective measures are not taken.**

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. This is why Exelon and other electric utilities take cyber security very seriously and have implemented strong cyber security programs to mitigate these risks.

Regardless of the scope of damages that any particular cyber security threat might inflict, owners, users, and operators of the bulk power system must also consider the potential consequences caused by any mitigation measures, such as potential impact to safe and reliable ongoing 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 owners, users, and operators to ensure that a measure aimed at protecting the grid from a malicious cyber attack does not instead cause other unintended and harmful consequences.

- **The costs and time required for mitigation of such risks.**

Many issues that may affect the overall security of the grid are not emergencies and thus do not need to be handled within hours or even days. 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 threat 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. Many, if not most, of the vulnerabilities the electric industry learns about are ranked as being a relatively "low" risk.

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 – as declared by the President or his designee.

- **How protection from cyber security breaches can be assured even as the electricity industry continues to evolve toward "smart grid" capabilities including greater use of digital information and controls.**

As grid technologies continue to evolve, 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 digitalization of the grid when it directed the Department of Energy to study these issues in Section 1309 of the Energy Independence and Security Act of 2007.

As new “smart grid” technologies are developed, it will be imperative for the industry to work closely with vendors and manufacturers to ensure they understand that cyber security is essential so that cyber security protections are incorporated into devices as much as possible.

It is equally critical that the architecture underpinning cyber security solutions for the grid and the architecture being developed for smart grid solutions are synchronized and compatible so that the smart grid solutions and the great benefits they will provide will be implemented in a secure fashion. With smart grid solutions in the early stages of development, opportunities exist to ensure this compatibility.

- **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.