Statement of
David K. Owens
Executive Vice President, Business Operations
Edison Electric Institute

Before the
Committee on Energy and Natural Resources
United States Senate

May 7, 2009

My name is David Owens, and I am Executive Vice President in charge of the Business Operations Group at the Edison Electric Institute (EEI). 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 percent of the ultimate customers in the shareholder-owned segment of the industry and represent about 70 percent of the U.S. electric power industry. I am accompanied by Steve Naumann, Vice President for Wholesale Market Development for Exelon Corporation. Steve also serves as Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC), and in his various roles he has more familiarity with the technical and operational aspects of cyber security issues related to the electric grid, as well as industry processes in place at NERC. We appreciate your invitation to appear today and the opportunity to testify about cyber security and critical electric infrastructure.

My testimony focuses on the nature of cyber security threats to the bulk electric power system, the efforts of electric utilities to respond to those threats, and the joint staff draft on critical electric infrastructure. I want to reassure the Committee that EEI's member companies and other owners, operators, and users of the bulk power system take cyber security very

seriously. Our companies deal with cyber security issues every day as one of many important aspects of grid reliability. Utilities have many processes and programs in place to protect their cyber infrastructure and mitigate the risks that cyber intrusions pose to reliable operations of their systems.

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.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. As cyber security threats continue to evolve and our cyber adversaries become more sophisticated, the private sector would welcome even more coordination with, and information from, government agencies with national security responsibilities that have the best access to intelligence concerning the nature of threats to electric utility systems. Electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and they understand how their complex systems operate. Electric utilities are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such an exploitation. 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.

As the industry relies increasingly on digital electronic devices and communications to optimize our systems and enhance reliability, cyber security will remain a constant challenge. Effective cyber security will continue to require a strong partnership among utilities, the federal government, and the suppliers of critical electric grid systems and components. Our companies believe they are up to their part of this task, building on our industry's historical and deep-rooted commitment to maintaining system reliability.

EEI member companies are addressing the risks they 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, they perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform companies about whether their preventive strategies are working so that they can enhance their protection as technologies and capabilities evolve. Penetration testing also allows them to practice and enhance their monitoring capabilities.

EEI members are also working with government partners—the national laboratories, the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Department of Energy (DOE), and the Office of the Director of National Intelligence (ODNI)—in many proactive programs to enhance the cybersecurity of the electric grid. For example, industry

participants worked with DOE to develop a strategic roadmap to identify and prioritize projects to enhance the security of electric industry control systems.

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 the Federal Energy Regulatory Commission (FERC) or DOE additional statutory authority should be limited to true emergency situations where there is a significant declared national security or public welfare concern. In

such an emergency, it is imperative that the government can 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.

A separate but equally important component of grid security is to ensure that manufacturers of critical grid equipment and systems are adequately fulfilling 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 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 digitization of the grid when it directed DOE 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 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.

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.

EEI agrees that it is appropriate for this Committee and Congress to consider legislation providing federal energy regulators new authority to address emergency cyber security threats. I want to emphasize, however, that current law already provides the means to address the many non-emergency cyber security issues in the electric industry. Section 215 of the Federal Power Act (FPA), which this Committee helped develop and which was enacted by Congress as part of the Energy Policy Act of 2005, provides for mandatory and enforceable electric reliability standards, specifically including standards to address cyber security, under FERC oversight. Chairman Bingaman and other Senators on this Committee should be commended for their work on enacting Section 215 and other efforts to ensure the reliability of the electric grid.

The basic construct of the relationship between FERC and NERC in developing and enforcing reliability standards 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. Any stakeholder, including FERC, may request that a standard be developed to address some aspect of reliability, expressly including cyber security.

I suggest the question on which the Committee should focus is, "What additional authority should be provided to federal energy regulators 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 FPA Section 215, and any new federal 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.

While the open stakeholder processes now used for developing industry-wide reliability and critical infrastructure protection standards admittedly are not well-suited to emergencies requiring immediate mandatory action with confidential handling of information, it is important to note that the vast majority of cyber security issues do not rise to the level of national security emergencies. Rather than creating broad new federal regulatory authorities that could undermine the consensus-driven policy framework developed through years of stakeholder input and memorialized in section 215, legislation should be focused on addressing a relatively narrow set of potential threats that legitimately merit special federal emergency authority.

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

Also, the joint staff draft provides DOE and FERC with parallel authorities to address cyber security threats and vulnerabilities, respectively. The joint staff draft could be clarified

and strengthened by providing for a single agency to take expedited actions based on advice or information from the President or intelligence agencies.

Federal legislation also should require that federal emergency cyber security orders end when the emergency is past or NERC has developed and FERC has approved a mandatory standard that handles the situation. The joint staff draft provides a 90-day "sunset" for emergency actions, unless FERC affirms or amends a rule or order after receiving comments.

Any cyber security legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. The complexities of keeping a large, interconnected system running safely cannot be understated. Consultation is critical to improving cyber security while maintaining safe and reliable utility operations. To the extent practicable, a basic premise of existing law—involvement of industry experts to develop mitigation measures— should be replicated for imminent cyber security threats. Cyber security legislation should provide reasonable opportunity for important industry consultation, without mandating a consultation that could delay implementation of mitigation in an urgent situation.

The consultation provisions of the joint staff draft are focused mostly on after-the-fact consultation with owners, users and operators. Without stronger requirements for prior consultation where possible under the circumstances, it is more likely that federally-ordered actions, developed under time pressure and without technical input from affected entities, could cause unintended adverse consequences to electric reliability.

It is also important to note that FERC has jurisdiction under FPA section 215 over owners, users, and operators of the bulk power system, the electric reliability organization (i.e.,

NERC), and regional reliability entities. The scope of this authority is relatively broad, including facilities and control systems that operate interconnected electric transmission networks and generation needed to maintain transmission reliability. However, the joint staff draft appears to represent a further broadening of federal regulatory authority that would extend to local distribution systems, which historically under the FPA has been reserved for the jurisdiction of state regulatory commissions.

Conclusion

While many cyber security issues are already being addressed under current law, we believe it is appropriate to provide federal energy regulators 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.

EEI and its member companies remain fully committed to working with the government and industry partners to increase cyber security. EEI's commitment to such coordinated efforts is illustrated by the broad representation of industry stakeholder associations represented on the joint statement on cyber security attached at the end of my testimony.

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

The North American Electric Power Industry's Top Priority is a Reliable and Secure Bulk Power System

The stakeholders of the electric power industry continue to work closely and in partnership with governmental authorities at the federal, state/provincial and local levels in both the United States and Canada in order to maintain and improve upon the high level of reliability consumers expect. Cyber security is an important element of bulk power system reliability that the electric power industry takes very seriously.

Electric Power Industry in Strong Partnership with Government

The electric power industry works closely with various government agencies on bulk power system security. On an ongoing basis, we communicate and collaborate in the United States with the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC), and in Canada with the various federal and provincial authorities to gain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including cyber security standards. In addition, NERC has an "alert and advisory" procedure that provides the electric power industry with timely and actionable information to assure the continued reliability and security of the bulk power system.

The Electric Power Industry Continuously Monitors and Acts Quickly to Ensure Bulk Power System Reliability and Security

Every day, the electric power industry continuously monitors the bulk power system and mitigates the effects of transmission grid incidents – large and small. Consumers and government are rarely aware of these incidents because of the sector's advance planning and coordination activities which reflect the quick and often seamless response the sector takes to address reliability and security events. This response includes prevention and response/recovery strategies – both are equally important. The industry's strong track record on reliability and security continues as we work diligently to adhere to **mandatory** NERC reliability standards, which are approved by FERC, including standards that address cyber security.

NERC Flexible Standards Approval Processes Meet Majority of Grid Challenges

NERC's industry-based and FERC-approved standards development process yields mandatory standards for the bulk power system that are clear, technically sound and enforceable, yet garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cyber-security, through consideration of the National Institute of Standards and Technology (NIST) framework for cyber-security, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also made important revisions to its standards development process by putting in place policies that allow, when necessary, for the confidential and expedient development of standards, including those related to cyber and physical security.

Emergency Cyber Situations Require an Expeditious and Efficient Approach

If the federal government has actionable intelligence about an imminent threat to the bulk power system, the electric power industry is ready, willing and able to respond. We understand it may be necessary for government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards. In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. As FERC, NERC and the electric power industry relationships move forward and mature in the area of reliability and security, any disruption of this would be counterproductive.

Improved Electric Power Industry-Government Partnership with Better Information Flow

In nearly all situations the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system. The electric power industry is fully committed to taking the needed steps to maintain and improve bulk power system reliability and security, and stands ready to work with Congress, FERC, other government agencies and NERC on these critical issues.

Supporting Associations and Contacts:

American Public Power Association	Joy Ditto	jditto@appanet.org
Canadian Electricity Association	Bonnie Suchman	bonnie.suchman@troutmansanders.com
Edison Electric Institute	Scott Aaronson	saaronson@eei.org
Electric Power Supply Association	Con Lass	Class@epsa.org
Electricity Consumers Resource Council	John Anderson	janderson@elcon.org
Large Public Power Council	Jessica Matlock	jdmatlock@snopud.com
National Association of Regulatory Utility Commissioners	Charles Gray	cgray@naruc.org
National Rural Electric Cooperative Association	Laura M. Schepis	laura.schepis@nreca.coop
Transmission Access Policy Study Group	Deborah Sliz	dsliz@morganmeguire.com