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 5, 2011

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 appreciate your invitation to discuss the cyber security of critical electric infrastructure and to comment on the Committee's draft legislation.

It is almost two years since I last had the opportunity to testify on this subject before this Committee. Since then, EEI's member companies—along with other owners, operators, and users of the electric grid—have continued to make cyber security a priority, while working together to make our critical infrastructure more resilient. In fact, EEI is part of a broader coalition of electric power stakeholders working on these issues. 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 unanimous support for a regime that leverages the strength of both the 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 our analysis of the Committee's bill, particularly as it relates to EEI's "*Principles of Cyber Security and Critical Infrastructure Protection*," which is attached for the record. This document was adopted by our Board of Directors last September in an effort to address cyber security threats and develop consensus around a framework to improve security for the electric grid. Included in this document, and most salient to the Committee's work today, are the following principles the industry believes are integral to successful cyber security policy:

- Leveraging public and private sector expertise, while including robust information sharing between government and the private sector, as well as among other stakeholders; and,
- A clear regulatory structure that focuses resources and attention on protecting truly critical assets from imminent threats.

Public-Private Coordination and Information Sharing

Among the myriad lessons learned following the earthquakes and tsunami in Japan is the need for dialogue and coordination *before* disaster strikes. It is clear that critical infrastructure protection is a shared cause that demands planning, as well as an understanding of roles and responsibilities ahead of time.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system. 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, the private sector can 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 or risk of a malicious 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 operated. 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 the Committee's draft bill acknowledges the need for intelligence sharing between government and the private sector, though we believe a more robust and explicit mandate is required.

It also is important to recognize that a strong industry partnership with government agencies currently exists. On an ongoing basis, the electric power industry communicates and collaborates in the United States with the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC). The industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including an array of "Critical Infrastructure Protection" or "CIP" standards. In addition, NERC, in its capacity as the Electric Sector Information Sharing and Analysis Center (ESISAC), uses its "alert and advisory" procedures to provide the electric power industry with timely and actionable information received from various federal agencies to assure the continued reliability and security of the nation's electric systems.

This NERC advisory system continues to evolve and, in the time since I last testified, has proven its ability to respond and disseminate information successfully when responding to significant national security events like the Stuxnet worm.

I would urge you not to reinvent the wheel, nor jump to conclusions about the efficacy of the existing cyber security regimes. The mechanisms in place to deal with these new and constantly evolving threats are, themselves, evolving. It is important that the Committee support continued participation in NERC's stakeholder-driven and FERC-approved standards and development process, which will yield mandatory CIP cyber security standards for the bulk power system that are clear, technically sound, and enforceable.

Finally, I would add that simply creating mechanisms for information sharing and public-private coordination 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.

Clear, Focused Regulatory Structure

A successful cyber security framework also needs to focus on protecting truly critical assets from imminent threats. There is a security axiom that states: if you try to protect everything, you protect nothing. Put another way, risk-based prioritization ensures both government and private sector resources are allocated wisely.

The distinction between imminent threats and vulnerabilities is an important one. Threats, by definition, constitute an emergency, while vulnerabilities might be exploited at a later date, providing time to determine the best way to respond to them.

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 the Electric Reliability Organization to establish 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. In approving such standards, FERC is to give "due weight" to the technical expertise of the ERO. 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. 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 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, 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 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 Committee draft provides DOE and FERC with parallel authorities to address cyber security threats and vulnerabilities, respectively. The Committee's 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.

To further focus efforts on those threats that have the potential to do the greatest harm, any new authority also should be limited to truly critical assets. Over-inclusion of electric utility infrastructure would be counterproductive; efforts to maintain and enhance the cyber security of the nation's critical electric infrastructure should focus first on the critical facilities that, if not protected, could cause substantial disruption to the nation's electric grid.

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.

Build Security into the Grid

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.

EEI is encouraging the development of a security certification program and expansion of National Lab involvement to provide independent testing for new grid components. Such a program would help utilities differentiate among different vendor solutions to select those that provide appropriate cyber security.

FERC "Interim Final Rule" authority

Under the Committee's draft legislation, FERC is to determine whether the current NERC reliability standards are "adequate to protect critical electric infrastructure from cyber security vulnerabilities." Under Section 224(b)(6)(C), any interim rule FERC enacts would stay in effect until NERC develops a reliability standard or modification that "the Commission determines provides adequate protection to critical electric infrastructure from the cyber security vulnerability addressed by the interim final rule."

Since NERC reliability rules apply only to the bulk electric system, FERC would have unilateral authority to write rules without input from the NERC stakeholder-driven process to establish technical standards. And, with no hearing or prior notice required before making the rule immediately effective, we are concerned about the lack of due process for stakeholder input. It would be desirable to at least have some requirement for FERC to consult with industry if time permits, similar to the consultation language in other parts of the bill.

FERC and DOE emergency procedure authorities

Having both FERC and DOE able to designate critical electric infrastructure introduces confusion and potential duplication. The lack of procedures or specific criteria for designating critical electric infrastructure is also problematic. It is unclear how, or if, an entity could challenge a designation by DOE under the general review provisions of the FPA.

Conclusion

With thousands of entities operating a single complicated, interdependent machine like the electric grid, the intra-industry coordination undertaken by the electric sector under the auspices of NERC has been invaluable.

There also are interdependencies not just within the electric sector, but across other critical infrastructure. For this reason, it would be preferable for Congress to take a comprehensive, multi-sector approach to legislation. 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. The interconnected nature of critical infrastructure prevents us from claiming victory unless a comprehensive approach is taken. I understand this Committee's jurisdiction and interest focus specifically on protecting the electric grid, but would urge you to work with the appropriate congressional committees to address cyber security more holistically.

That said, while many cyber security issues already are 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.

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 coalition of industry stakeholder associations that continue to work together on these matters.

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

EDISON ELECTRIC INSTITUTE

September 9, 2010

EEI Principles for Cyber Security and Critical Infrastructure Protection

Background

Protecting the nation's electric grid and ensuring a reliable supply of power is the electric power industry's top priority. Cyber security incidents may disrupt the flow of power or reduce the reliability of the electric system. Key to the success of this effort is the ability to provide measures capable of protecting the evolving intelligent network against interruption, exploitation, compromise or outright attack of cyber assets, whether the attack vector is physical, cyber or both.

The electric power industry takes cyber security threats very seriously. As part of the industry's overall reliability effort, electric companies work to maintain the reliability and the security of the computers, control systems, and other cyber assets that help electric companies operate the electric grid. In response to the cyber threat, electric companies employ various strategies to protect these systems, but cyber security threats still exist.

Addressing Cyber Security Threats

Reliability is more than a slogan for the electric utility industry - it's a mandate. In fact, federal and state regulators have significant interest and statutory authority in ensuring electric companies provide adequate reliability. Thus, utilities take very seriously their responsibility to address cyber vulnerabilities and the security of the computers, control systems, and other cyber assets that help operate the electric grid. This focus on reliability, resiliency and recovery takes into account an all-hazards approach, recognizing risks from natural phenomena such as hurricanes or geomagnetic disturbances to intentional cyber attacks.

Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, and the suppliers of critical electric grid systems and components. Electric companies work closely with the North American Electric Reliability Corporation (NERC) and federal agencies to enhance the cyber security of the bulk power system. This includes coordination with the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), as well as receiving assistance from federal intelligence and law enforcement agencies.

To complement its cyber security efforts and to address rapidly changing intelligence on evolving threats, the industry embraces a cooperative relationship with federal authorities to protect against situations that threaten national security or public welfare, and to prioritize the assets which need enhanced security. A well-practiced, public-private partnership utilizes all stakeholders' expertise, including the government's ability to provide clear direction and assess threats, while owners and operators of the critical infrastructure propose mitigation strategies that will avoid significant adverse consequences to utility operations or assets. At the same time a constructive regulatory environment will assure that incremental investments to protect the grid are prudent, and reduce risk in a manner proportional to the cost.

Protecting the Grid is a Shared Responsibility

1. Prioritize Assets to Ensure Effective Protection

Recognizing that there are a variety of interdependencies, and potential consequences associated with the loss of different facilities, the utility industry supports a risk-based, prioritized approach that identifies assets truly critical to the reliable operation of the electric grid. This ensures the most important elements of our system receive the highest level of attention, as well as the resources necessary to secure them.

2. Threats Require Emergency Action; Vulnerabilities Should Be Addressed More Deliberately

In this context, a threat is imminent and requires a rapid response. In these instances, the industry is willing to accommodate certain operational consequences in the interest of addressing the threat. Vulnerabilities, on the other hand, have a longer time horizon and can benefit from a more measured response. Government authority should reflect and respect these different levels of danger.

3. Clear Regulatory Structure and Open Lines of Communication

The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. It is critical that the federal government and industry communicate with each other seamlessly; to avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action.

4. Proactively Manage New Risks

As the new Smart Grid develops, it is essential that cyber security protections are incorporated into both the grid architecture and the new smart grid technologies. The electric power industry must continue to work closely with vendors, manufacturers, and government agencies and be aligned with emerging and evolving cyber security standards (such as those being driven by NIST) to ensure that the new technology running the grid is, most importantly, secure and reliable. We encourage the development of a security certification program that would independently test smart grid components and systems and certify that they pass security tests. This certification process would help utilities select only those systems that provide appropriate cyber security.

5. Committed to Protecting Bulk Electric System and Distribution Assets

The utility industry understands that cyber attacks affecting distribution systems could have broader implications. Since jurisdiction is split between state regulators and the Federal Energy Regulatory Commission, the utility industry supports enhanced threat information coordination and communication between regulatory agencies and utilities to protect our systems (whether distribution or the bulk electric system) while also honoring the existing regulatory model.

6. Cost Recovery and Liability Protection

Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.

The **Edison Electric Institute (EEI)** is the association of U.S. Shareholder-Owned Electric Companies. Our members serve 95 percent of the ultimate customers in the shareholder-owned segment of the industry, and represent approximately 70 percent of the U.S. electric power industry.

We also have more than 70 international electric companies as Affiliate Members, and nearly 200 industry suppliers and related organizations as Associate Members.

Organized in 1933, EEI works closely with all of its members, representing their interests and advocating equitable policies in legislative and regulatory arenas.

EEI provides public policy leadership, critical industry data, market opportunities, strategic business intelligence, one-of-a-kind conferences and forums, and top-notch products and services.

For more information on EEI programs and activities, products and services, or membership, visit our Web site at www.eei.org.

EDISON ELECTRIC INSTITUTE

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2696
202-508-5000
www.eei.org