Statement

Of the

SACRAMENTO MUNICIPAL UTILITY DISTRICT

For the

HOUSE ENERGY AND ENVIRONMENT SUBCOMMITTEE'S

Hearing Entitled "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195"

October 27, 2009

Introduction

The Sacramento Municipal Utility District (SMUD) appreciates the opportunity to provide the following testimony for the hearing entitled "Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195." I am John DiStasio, General Manager and CEO of SMUD.

SMUD has been supplying electricity to California's capital region since 1946. SMUD serves a population of 1.4 million and has 473 miles of transmission lines and 9,784 miles of distribution lines crossing its service territory of 900 square miles. SMUD's 594,595 residential and business customers include such large accounts as the State of California, the County of Sacramento and Intel. A number of SMUD's customers – including the State of California, Regional Sanitation and local hospitals – are critical to public welfare and economic security.

SMUD is a member of the American Public Power Association (APPA) and the Large Public Power Council (LPPC), both of which are part of a larger coalition of electricity stakeholders that have been working together on the cyber security issue in the legislative arena for the last two years and on grid reliability issues for decades.

The associations in our industry coalition represent a broad variety of stakeholder interests, including investor-owned, cooperatively-owned and publicly-owned utilities, independent generators, Canadian utilities, large industrial consumers, and state public utility commissions. (Although the Subcommittee has invited the National Association of Regulatory Utility Commissioners (NARUC) to testify separately, it is important to note that they are also a part of this broad industry coalition.) For legitimate reasons, we usually have very different views on the policy issues facing our industry. On the issue of protection of the bulk power system from cyber security threats and addressing cyber security vulnerabilities, however, we have been working together in recent years to help develop the North American Electric Reliability Corporation's (NERC) reliability standards for critical infrastructure protection and more recently, in the last two years, on identifying areas where additional legislation may be needed. APPA, LPPC, NARUC, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group all support carefully crafted and specific legislation to deal with the discrete issue of cyber security. We understand the seriousness of the issue, and the need to deal with it. At the same time, we believe that such legislation must be carefully drawn and narrow in its application, to avoid disrupting the mandatory reliability regime that Congress has already required and the electric utility industry is implementing, with oversight by the Federal Energy Regulatory Commission (FERC).

It is extremely important for the Subcommittee to understand that it is in the industry's best interests to protect against cyber security attacks. From the electric utility standpoint, when the lights go out, for whatever reason, we are the ones held responsible. We do not want the lights to go out for any reason, but if and when they do, we want to

be able to bring them back on as quickly as possible, to minimize the potential risks to health, safety, and property, and to minimize the adverse financial impacts on the public. At the same time, our industry is facing additional regulatory requirements in a number of areas, which all translate into increased costs to the consumer. Therefore, it is imperative that we use our dollars and workforce wisely to address the threats and vulnerabilities in the cyber security realm that are most likely to occur, and have the greatest potential impact. This is best accomplished by close collaboration between the government and industry participants rather than "finger pointing" and distrust.

Attached to my testimony is a two-page issue brief that outlines this common perspective among the electric power trade associations, setting out certain shared principles we all support.

Cyber Security Principles

SMUD and the industry coalition believe that legislation regarding the cyber security of the nation's electric power system should be based on certain core principles, and take into account cyber security protection efforts already underway. Any legislation Congress adopts should:

(1) *Continue the strong industry partnership with government agencies in the United States and Canada*. 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 FERC. Similarly, in Canada, the industry deals with the various federal and provincial authorities to obtain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with NERC to develop mandatory reliability standards, including an array of cyber security standards, which NERC calls "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 participants in 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. (The ESISAC was established in 1998 in advance of the Y2K issue, and has functioned well since, as noted in NERC's written testimony for today's hearing.) NERC has adopted important improvements to its ESISAC alert communications software that will allow more targeted communications and provide for a more secure, reliable two-way communications pathway between NERC and industry members.

For example, during the Conficker worm outbreak, NERC issued the first alert on October 24, 2008, immediately after Microsoft detected the worm and released its advisory. The alert from NERC included actionable procedures for utilities to implement in order to mitigate the threat of Conficker. As Conficker mutated, NERC issued several updated advisory notices. SMUD and other utilities were

provided with early warning communications containing the information about the threat, which permitted us to implement the control and counter-measures that were appropriate for our utility operations.

(2) *Foster the current electric power industry-wide commitment to continuously monitor the bulk power system and mitigate the effects of transmission grid reliability and security incidents, including cyber security incidents, large and small.* All sectors of the industry are working to instill a culture of compliance with NERC's mandatory electric reliability standards, which are enforced by NERC and FERC within the United States. Maintaining and enhancing the cyber security of our bulk power control and communication systems is a fundamental element of this developing industry culture. The electric utility industry is unlike many other critical infrastructures in the United States, in that each utility company, whether publicly or privately owned, is physically interconnected with and directly affected by the operating practices of its neighboring utilities. This is so because the nation's electric system is interconnected, electricity must be generated and used instantaneously based on the laws of physics, and since electrons follow the path of least resistance as they flow through the system. The very fact that our actions can adversely affect the reliable operation of our neighbors gives the industry a shared responsibility and commitment to reliability and to mandatory and enforceable reliability standards. We are acutely aware that the need to maintain and enhance cyber security presents a new set of potential challenges and opportunities to the industry.

New operational applications made possible by "smart grid" technologies, for example, also may present new vectors for attack upon both new and existing utility systems. On the other hand, manufacturers need to design and utilities need to use smart grid applications that provide new ways of detecting and responding to malicious activity on the electric grid. In addition, the key issue with new "smart grid" devices, either at the bulk transmission level or at the distribution/consumer level, is the manner in which they are developed and manufactured. The electricity industry is involved in the standards development process at the National Institutes of Standards and Technology (NIST) being undertaken to address these new technologies. One key issue is the ways in which these devices communicate. We would suggest that the design should enable communication with a centralized energy management system, similar to the way in which online banking allows communication between an individual and the financial services center, but not among other individuals. This would mean that the energy management system would be the primary place where state of the art cyber security is installed, rather than at the terminus of millions of customers' connections (although some level of security will be needed on the user side as well, again similar to online banking). This is more of a "hub and spoke" approach, and one with which utilities are very familiar. It is also a common risk management strategy – segmenting of networks to minimize risk. Smart grid overlays ought to be segmented to minimize risk exposure to the central "brain."

In response to NERC's Critical Infrastructure Protection Standards, CIP-002 through 009, electric utilities are actively engaged in securing their energy management centers, both physically and electronically. Physical security is being enhanced to institute a six-wall security perimeter, while electronic protection measures include: vulnerability assessments; the securing of access points through firewalls; active monitoring of access points; extensive use of anti-virus and malware protection software; and stronger authentication methodologies. There is also a widespread effort to install complete backup systems in secondary facilities.

(3) *Support continued participation in NERC's industry-based and FERC-approved standards development process, which will yield mandatory cyber security standards for the bulk power system that are clear, technically sound and enforceable, which garner broad support within the industry, and which can be implemented in both the U.S. and Canada on the interconnected North American Transmission Grid.* NERC is striving to draw from the state-of-the-art cyber security controls and countermeasures, through consideration of the NIST framework for cyber security, and to integrate that framework into NERC's existing cyber security standards. NERC, as an organization, and the industry have made a significant commitment of resources to the development of revised and new cyber security standards. In fact, we have committed some of our scarcest resources – our subject matter experts in cyber security and system operations – to the task of developing "second generation" draft standards for consideration by the industry as a whole. NERC has also made important revisions to its standards development process, by putting in place policies that allow, when necessary, for the confidential and expedited or emergency development of reliability standards, including those related to cyber security.

(4) *Be limited to the realm of cyber security.* Some would prefer to include in cyber security legislation "other national security threats" in addition to cyber security threats. SMUD and the industry coalition believe that other government entities, both state and federal, have more direct responsibilities in the general area of national security. Moreover, the electric utility industry has been addressing physical threats since its inception over 100 years ago through existing communication lines between law enforcement agencies at the local and federal levels as well as through its own security measures. SMUD has established strong and long-term partnerships and communications with the Federal Bureau of Investigation (FBI) and Local Law Enforcement Agencies (Sacramento County Sherriff's Department, El Dorado County Sheriff's Department, and Sacramento City Police Department) to aid in response and investigations to Physical Security Incidents or Threats to the Electrical Infrastructures.

SMUD is actively involved and/or part of industry groups that share information and tour facilities to help identify best practices, such as the Edison Electric Institute (EEI) and the

Western Energy Coordinating Council (WECC) Physical Security Working Group (PSWG).

SMUD is actively involved in leadership positions on boards such as the FBI InfraGard Program in which we receive a broad spectrum of information across all of the nation's critical infrastructures as determined by the Department of Homeland Security (DHS). We also have direct contacts with the Regional Terrorism Threat Assessment Center (RTTAC), DHS Office, Office of Homeland Security (OHS – California).

SMUD along with these local law enforcement agencies (LLEA) have conducted numerous Buffer Zone Protection Plans (BZPP) and Security and Vulnerability Risk Assessments of Critical Infrastructures to identify additional measures to better protect these facilities from sabotage or terrorism events.

SMUD's program also consists of effective communications with FERC, NERC and WECC and membership with the Electric Sector Information Sharing and Analysis Center (ESISAC). As a result of our strong partnerships and open lines of communication with these entities, SMUD receives information, key communication and support pertinent to effective protection of our employees, assets and critical infrastructures.

SMUD has established and tested policies, procedures, checklists and training of its personnel to effectively respond and communicate to management and LLEA regarding threats, sabotage, terrorism events and situations as reflected in our preparation for Y2K, 911, and Homeland Security Threat Level Upgrades, etc.

The Subcommittee has also asked me to address electromagnetic phenomena that could affect physical assets. One such phenomenon is a geomagnetic storm. This is solar wind that penetrates the earth's atmosphere and, through the motion of charged ions, induces a direct current on long alternating current lines and can impact the reliability of the grid. Electric utilities that operate in northern latitudes are particularly vulnerable to such geo-magnetic storms. Such phenomena have nothing to do with cyber security, and have existed since the electric grid's inception, as have other types of natural phenomena like catastrophic storms. What we do to address these infrequent types of events is to create redundancies in the system, strengthen key parts of the grid, and establish plans and protocols for restoring electric service. SMUD has established confidential plans and protocols for recovering the electric system in the event of a failure – in fact, we have the ability to reenergize the SMUD system in the event of total collapse of the electric grid. This involves a complex, confidential plan that is comprised of specialized generating units and specific operating procedures that will allow SMUD to begin reenergizing select transmission lines and restoring electric service in a systematic way following a grid catastrophe. WECC and NERC have independently audited our plans and have certified that SMUD meets the requirements to provide this capability.

Another type of electromagnetic pulse can be caused by a nuclear bomb exploding at a high altitude, which cannot be prevented by electric utilities. We depend on the federal

government and military to prevent such an attack. However, NERC has recently established a task force in coordination with DOE to assess realistic measures that can be taken to mitigate risks of outages and equipment damage from this and other high impact, low frequency events.

There are four specific areas in which SMUD and the industry coalition support additional statutory authorities for the federal government and in particular for FERC and DOE:

(1) *Narrowly targeted authority for the FERC to issue emergency orders in response to an imminent threat to the bulk power system.* If the federal government has actionable intelligence about an imminent threat to the bulk power system, and time does not allow for classified industry briefings and timely development of mitigation measures for such a threat, FERC, following consultation with the appropriate governmental authorities in Canada, should be authorized to direct the electric power industry to take needed emergency actions. The electric power industry is ready, willing and able to implement targeted mitigation measures that are clearly linked to the nature of the underlying threat. However, these emergency directives should provide utilities the ability to implement controls related to their operating environment and only remain in effect until the threat subsides or FERC approves related NERC-developed reliability standards that establish permanent measures to address the specific threat. In the United States, Section 215 of the Federal Power Act (added by the Energy Policy Act of 2005) invested FERC with a significant supervisory role in bulk power system reliability. It would be inefficient and confusing to provide potentially duplicative responsibilities to another agency. But at the same time, it would be highly disruptive to the NERC process for development of mandatory and enforceable electric reliability standards set out in FPA Section 215 for the FERC to impose permanent or quasi-permanent cyber security standards that have not undergone the due process steps within the industry required by that section. Further, given that Canadian authorities have already approved NERC's current CIP standards, inconsistent standards in the U.S. and Canada could undermine reliability and potentially make the North American grid more vulnerable to a cyber attack. H.R. 2165 appropriately designates a process for FERC to issue such directives in a cyber emergency.

(2) *Specific authority for the Commission to issue orders that address certain vulnerabilities to the bulk power system identified in the June 21, 2007, ESISAC Advisory issued by NERC, and related remote access issues*. FERC should be authorized to direct that remedial measures be taken by United States entities subject to NERC reliability standards. H.R. 2165 authorizes FERC to carry out such remedial measures. It is important to note that in the two years since the Aurora vulnerability was identified, the industry has taken steps to address the issue, and no cyber attack has occurred similar to the incident the Aurora exercise was intended to simulate.

(3) *Improved communications flows of timely and actionable information from government to industry, matched by enhanced responsibility for the electric power industry to share critical energy infrastructure information with government agencies on a similarly secure and confidential basis.* The industry welcomes secure communication and collaboration with government agencies and the exchange of intelligence information on a particular cyber security threat or vulnerability. It is critical that such information be timely, specific, and actionable as to the nature of the threat or vulnerability to which the utility industry is exposed. After receiving this information, the electric power industry could then direct its expert operators and cyber security staff to take the necessary steps to secure systems and networks, ensuring the reliability and security of the bulk power system. However, it is important to understand that the experts in the utility sector are currently not granted the necessary security clearances to obtain this actionable intelligence information from government and to act as "translators" between the government and the industry with regard to the most effective actions to be taken to secure the grid. We would urge the Subcommittee to consider this issue as the legislation further develops.

While a number of federal agencies have roles in the existing communication process, SMUD and the industry coalition support placing DOE in the role of the lead agency in communicating threat information to the electricity sector because of DOE's decades-long interaction with and understanding of the electric utility industry.

(4) *Enhanced authority for the electric power industry to protect and keep critical energy infrastructure information confidential and non-public.* The electric power industry and government face a variety of complex issues associated with the non-public exchange of Critical Energy Infrastructure Information (CEII) as well as gaining appropriate access to highly sensitive cyber security threat and vulnerability information available to government agencies. For example, NERC and FERC face conflicting statutory obligations to use open, public stakeholder processes to develop cyber security standards and to approve such standards through public notice and comment, while safeguarding from public disclosure threat and vulnerability information that may provide the rationale for certain elements of these reliability standards. Public power utilities like SMUD face their own unique problems in this area. As instrumentalities of state and local governments, public power utilities are subject to state public record and open meeting laws, which make keeping a variety of information non-public more difficult. As publicly-owned entities, this is as it should be – public power utilities are committed to open government and transparency. However, in the case of CEII, transparency is not in the public interest. Just as certain federally-owned utilities may face difficulties protecting information from Freedom of Information Act (FOIA) requests, even when CEII protections are invoked, state and locally-owned utilities face the risk of state record requests for such information. The transfer of such sensitive information to a non-governmental third party makes protection of CEII for public power systems even more

difficult. APPA has developed language to address this issue that we hope will be included as the process moves forward. H.R. 2165 addresses the other areas delineated above.

(5) *Be limited to the bulk power system.* Congress established the Section 215 mandatory reliability structure in recognition that threats to the nation's bulk power system, if actuated, were much more likely than threats to individual distribution systems to create significant effects on national security and our economic interests. This is still true today. Where distribution utilities are interconnected and material in some way to the reliability of the bulk power system, those assets are included in the NERC Compliance Registry.

For a variety of reasons, some policy makers now suggest that physical and cyber assets of distribution utilities must be included in a new iteration of mandatory reliability regulation. They have cited the service of financial and military centers by distribution systems. Some believe that attacks on distribution systems can easily move upstream and impact the bulk power system. Others see the "smart grid" as creating insurmountable numbers of vulnerable system components.

The nature of a load does not alter the fundamental nature of utility operations and the protections built in between distribution components and the bulk power system. Utilities reliably served critical economic and military customers at the time Section 215 was created and implemented. Individual utilities continue to work closely with their critical loads to ensure they are providing the level of service and protection that these customers require. These local, customer-specific relationships provide the foundation for handling threats and vulnerabilities that are targeted against critical customers.

SMUD and the industry hope that Congress will recognize that "critical customers" are not all alike. Many high-tech companies require an extremely high level of service reliability and power quality that cannot be provided from the electric grid alone. On site power conditioning equipment, multiple distribution feeds and even redundant local generation is needed to protect server farms from even momentary interruptions. These customers can and do pay for this superior "five-nines" level of service. Many military bases also require a highly secure power supply, but this supply may or may not require the same level of power quality for the entirety of a particular base's load. A large military base will typically have its own distribution network and may have its own backup generation, complete with an on-base supply of distillate fuel.

Of course, no system – or customer - can be 100 percent secured, but utilities are consistently focused on maintaining a robust level of system protection against any and all threats. Without prompting through legislation, utilities follow a core business practice often called "defense in depth." This means there are protection plans in place in multiple locations between distribution facilities and the bulk power system. For example, utilities use firewalls, intrusion prevention and detection devices and warning systems to deter, prevent and report system

incidents. The utility industry continues to provide its experiences as informed by decades of deploying "defense in depth" strategies when helping to create NERC cyber standards and in implementing them. Utilities are not abandoning their commitment to protect their systems as the smart grid evolves toward integration into the overall utility infrastructure.

Finally, this defense in depth includes recognition that the electric utility industry faces threats to continuity of service on a continuous basis, from small local events such as copper theft from substations and lightning strikes on utility poles, to major regional events such as hurricanes and ice storms. Through our voluntary mutual aid networks, the industry has become quite adept at putting the electric grid back together after such events. After major storms, we share electrical equipment, poles and personnel to get the lights back on as quickly as possible. Federal government assistance is critical during this restoration process, not to lead the effort, but to make sure during major disasters that the electric utility industry and its contractors have timely and preferred access to other infrastructures that are needed to speed restoration.

Additional Comments on H.R. 2165, H.R. 2195, and the Language on Cyber Security Included in Title III, Subtitle A, of S. 1462

SMUD and the industry coalition support H.R. 2165 because it best delineates the necessary new process for the federal government to interact with the industry in the event of a cyber security emergency while not disrupting the existing regulatory structure set forward in Section 215 of the Federal Power Act. In terms of the other legislation that the Subcommittee has asked us to review, SMUD and the industry coalition have some concerns with H.R. 2195 and the cyber security title of S. 1462, including the following:

Inclusion of potentially all electric utility industry assets, including distribution, is overly broad in both H.R. 2195 and S. 1462.
Both define "Critical electric infrastructure" to include distribution systems and assets that if incapacitated or destroyed would have a debilitating impact on national security, national economic security, or national public health or safety. Depending on how FERC and DOE make their respective determinations in implementing the statute, virtually all electric utility infrastructure could be included within the scope of this new statutory authority, even infrastructure in Canada. SMUD and the industry coalition believe that over-inclusion of electric utility infrastructure would be counterproductive; by attempting to protect everything, efforts to protect the truly critical and important infrastructure would be diluted. SMUD and the industry coalition therefore support targeting new FERC and DOE authority toward imminent cyber security threats to the bulk power system in the United States, rather than the broader universe of facilities envisioned in H.R. 2195 and S. 1462. These bills could expose over 1,000 additional distribution systems to FERC and DOE regulation imposing very substantial regulatory and financial burdens on many small cities, towns, and rural areas that are disproportionate to the limited cyber security risks that these facilities and entities pose to the bulk power system, if any. Further, the amount of distribution facilities operated by electric utilities

in the United States vastly exceeds the transmission grid. Platts' 2009 UDI Directory of Electric Power Producers and Distributors reports that there are over 5.8 million miles of distribution lines in the United States (compared to 611,000 miles of transmission lines).

Again, SMUD and the industry coalition believe that the effort to maintain and enhance the cyber security of the nation's critical electric utility infrastructure should focus first on the critical facilities and systems that, if not protected, could contribute to disruption of the nation's power supply.

FERC discretion appears to be broad and unfettered in H.R. 2195 and S. 1462.
Both bills *direct* FERC to issue rules and orders to protect critical electric infrastructure from cyber security threats. This directive imposes no real limits on the extent of FERC authority to order specific actions. As written, it appears that FERC could order the enlargement of facilities, interconnections or disconnections or any other action it deems necessary, without any obligation even to consult with the industry in advance to determine whether its proposed course of action is the most effective and cost-efficient way to address a particular threat. This provision (similar in both bills) would also permit FERC to issue cyber security orders that directly replace or supplement industry- and FERC-approved reliability standards, undermining the carefully crafted reliability regime set out in Section 215. H.R. 2165 allows FERC to take action without obviating the Section 215 and NERC standards development process.

FERC and DOE emergency procedure authorities are potentially redundant in S. 1462.
In S. 1462, FERC and DOE are *both* granted authority to act on an emergency basis without prior notice or hearing for up to 90 days, with FERC authorized to take expedited measures to protect critical electric infrastructure from cyber security vulnerabilities and DOE authorized to take emergency actions to protect critical electric infrastructure from cyber security threats. SMUD and the industry coalition suggest that such emergency or expedited authority be assigned to a single agency, to avoid duplication and confusion as to the respective roles of the two agencies. It is imperative that agency directives not be conflicting.

The requirements to consult with industry and to mitigate burdens before directives become effective should be stronger in both H.R. 2195 and S. 1462.
FERC's authority to issue rules or orders in both bills presumably is subject to the judicial review procedures set out in the FPA, as well the Administrative Procedures Act (although these points should be clarified). DOE and FERC authorities to issue emergency orders in S. 1462 and H.R. 2195 are subject to a 90 day sunset unless FERC "gives interested persons an opportunity to submit written data, views, or arguments . . ." Unfortunately, there is no requirement in either bill for FERC (and DOE, in the case of S. 1462, and DHS in the case of H.R. 2195) to consult with the industry in advance, even as time permits, regarding the nature of the threat or vulnerability, or to take into account the industry's views on the most efficient way in which to address the threat and/or methods for reducing the associated burden on the industry. Moreover, the filing of a request for rehearing or petition for review would not stay the effectiveness of the

directive. Compliance with a potentially flawed directive would therefore be both mandatory and subject to financial penalties under FPA Section 316A (EPAct Sec. 1284).

H.R. 2195 and S. 1462 do not fully address confidentiality issues, including the need for processes governing non-public communications between FERC/DOE and the industry, and the particular confidentiality issues faced by public power utilities. As discussed above, a variety of other communications may need additional safeguards. As noted previously, H.R. 2165 contains provisions that deal with these somewhat complex confidentiality concerns in a more comprehensive and effective manner than do H.R. 2195 and S. 1462, although the latter bills' correctly identify the issue as problematic and could be modified to address industries' concerns. SMUD would also still ask to work with the Subcommittee on some specific concerns relating to state and local sunshine laws that affect public power entities that are not fully addressed in H.R. 2165.

In summary, SMUD and the industry coalition believe the language included in H.R. 2165 properly addresses the necessary, but limited, scope of new federal regulation to address imminent cyber security threats on the bulk power system.

Thank you for the opportunity to present SMUD's and the industry's views on the important cyber security issues facing the electric utility industry. We look forward to continuing to work with the Subcommittee on this important issue and we are available to provide any further assistance.