American
Public Power
Association

1875 Connecticut Avenue, NW
Suite 1200
Washington, DC 20009-5715

Ph: 202.467.2900
Fax: 202.467.2910
www.APPAnet.org

Statement

Of the

AMERICAN PUBLIC POWER ASSOCIATION (APPA)

For the

SENATE ENERGY AND NATURAL RESOURCES COMMITTEE'S

Hearing Regarding Joint Staff Draft Related to Cyber

Security and Critical Electricity Infrastructure

May 7, 2009

Introduction

APPA appreciates the opportunity to provide the following testimony for the Senate Energy and Natural Resources Committee's hearing regarding the Joint Staff draft related to cyber security and critical electricity infrastructure. I am Allen Mosher, Senior Director of Policy Analysis and Reliability for APPA.

APPA represents the interests of more than 2,000 publicly-owned electric utility systems across the country, serving approximately 45 million Americans. APPA member utilities include state public power agencies and municipal electric utilities that serve some of the nation's largest cities. However, the vast majority of these publicly-owned electric utilities serve small and medium-sized communities in 49 states.

My comments concerning the electric utility industry's work on cyber security issues and the Joint Staff draft that is the subject of today's hearings are offered on behalf of APPA alone. I would be remiss, however, if I did not first discuss the broad consensus within the electric power industry in support of enhanced, albeit narrowly targeted, authorities for the Federal Energy Regulatory Commission (FERC) and the United States Department of Energy (DOE) in the area of cyber security.

The associations in our industry 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. For very legitimate reasons, we usually have very different views on the policy issues facing our industry. On the issue of protection of the electric bulk power system from cyber security

emergencies, however, we have been working together for over a year. APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility Commissioners, 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 emergencies. 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 FERC oversight.

Attached to my testimony is a two-page issue brief that outlines this common perspective among the electric power trade associations in support of certain shared principles. However, I must emphasize that this testimony is provided solely on behalf of APPA. I will also address APPA's initial assessment of the Joint Staff draft, although these views are only those of APPA Staff, since we were unable to review the draft legislation with APPA's members prior to the filing of this testimony.

APPA Cyber Security Principles

APPA believes legislation regarding the cyber security of the nation's electric power system should be based on certain core principles, and take into account efforts now 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, DOE and FERC. Similarly, in Canada, the industry deals 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 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 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. NERC is in the process of adopting 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.

(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, large and small.* All sectors of the industry are working to instill a culture of compliance with mandatory electric reliability standards enforced by the Commission 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 interconnected with and directly affected by the operating practices of its neighboring utilities. The very fact that our own actions can adversely affect the reliable operation of our neighbors gives the industry a shared commitment to reliability and to mandatory reliability standards. The need to maintain and enhance cyber security, coupled with the deployment of complex digital communications networks for system control, presents a new set of potential challenges and opportunities to the industry. New efficiencies made possible by smart grid for example, also present new vectors for attack upon both new and existing system control networks that could present a risk of cascading outages. On the other hand, it may be possible to design smart grid applications that provide new ways of detecting and responding to malicious activity on the electric grid.

(3) *Support continued participation in NERC's industry-based and FERC-approved standards development process which will yield mandatory CIP cyber security standards for the bulk power system that are clear, technically sound and enforceable, and which 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's (NIST) framework for cyber security, and to integrate that framework into NERC's existing Critical

Infrastructure Protection standards. As Vice Chairman of the NERC Standards Committee, I can personally attest that both NERC, as an organization, and the industry have made a significant commitment of resources to the development of new cyber security standards. In fact we've committed some of our scarcest resources – our subject matter experts in cyber security and system operations – to the task of developing 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.

However, there are four specific areas in which APPA would 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, or a newly identified vulnerability on, the bulk power system, and time does not allow for classified industry briefings and timely development of mitigation measures for a threat or vulnerability, the FERC in the United States and the appropriate corresponding 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 respond to specific directives based on targeted mitigation measures that

are clearly linked to the nature of the underlying threat. However, these emergency directives should only remain in effect until the threat subsides or FERC approves related NERC-developed reliability standards that establish permanent measures to address the specific vulnerability that the threat was intended to exploit. 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 duplicative and inefficient to recreate that responsibility at another agency. But at the same time, it would be highly disruptive to the 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.

(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.* In APPA's view, the vulnerabilities identified in the so-called "Aurora Advisory" can and will be addressed through the development of new NERC cyber security standards for the bulk power system that will be posted for industry comment. These standards will be comprehensive in scope and will encompass all bulk power system asset owners, operators and users in various degrees. The standards will address the potential underlying vulnerability by securing utility assets from unauthorized remote access. Until such time as those standards are adopted, however, FERC

should be authorized to direct that remedial measures be taken by United States entities subject to NERC reliability standards.

(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.* In normal circumstances, 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 cyber security threat or vulnerability, it is critical that such information be timely and actionable. After receiving this information, the electric power industry can 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. While a number of federal agencies have roles in this communication process, APPA continues to support placing DOE in the role of the lead agency in communicating threat information to the electricity sector as well as to other sectors of the energy industry. DOE's understanding of the electric utility industry provides it with the ability to filter and translate intelligence information into a more actionable form. Moreover, because DOE does not have direct regulatory authority over the electric utility industry, it will be better situated to receive candid assessments of potential industry vulnerabilities or attempts to penetrate electric power industry assets than FERC,

which is charged with enforcing industry compliance with mandatory reliability standards, with penalties of up to $1 million per day for each violation.

(4) *Enhanced authority for the electric power industry – particularly public power utilities – 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 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 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 third party makes protection of CEII for public power systems even more difficult. Public power systems are currently developing possible statutory approaches to address their unique CEII concerns. APPA notes that H.R. 2165, introduced on April 29, 2009, by Rep. John Barrow (D-GA) and co-sponsored by Energy and Commerce Chairman Henry Waxman (D-CA) and Rep. Ed Markey (D-MA), contains provisions intended to address these pressing information disclosure issues. While APPA has not completed its analysis, H.R. 2165 appears to comport with many of the points I have laid out in this testimony, including the need for enhanced authority to protect CEII.

APPA Staff Comments on Joint Staff Draft

APPA staff has also reviewed the Senate Energy and Natural Resources Committee Joint Staff draft of proposed Federal Power Act Section 224, which would authorize FERC and DOE to issue rules and orders to respond to cyber security vulnerabilities and threats to critical electric infrastructure. While we appreciate the Committee working to address this important issue, APPA does have some concerns with that draft, including the following:

Inclusion of potentially all electric utility industry assets, including distribution, is overly broad.

Sec. 224 (a)(1) defines "Critical electric infrastructure" to include distribution systems and assets that if incapacitated or destroyed would have a debilitating impact on 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. APPA believes 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. APPA therefore supports targeting new FERC and DOE authority toward urgent cyber security threats to the bulk power system, rather than the broader universe of facilities envisioned in the Committee staff draft. The Committee staff draft could expose over 1,650 additional public power distribution systems to FERC and DOE regulation, imposing very substantial regulatory and financial burdens on many small cities and towns that are disproportionate to the potential cyber security risks that these entities pose. Again, APPA believes 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 cause substantial disruption to the nation's electric utility industry.

FERC discretion appears to be broad and unfettered.

Sec. 224 (b)(1) *directs* FERC to issue rules and orders "*as are necessary* to protect critical electric infrastructure from cyber security threats." [Emphasis added.] This section 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 section would also permit FERC to issue cyber security orders that directly replace or supplement industry-approved reliability standards, undermining one of the fundamental tenets underlying Section 215.

FERC and DOE emergency procedure authorities are potentially redundant.

Under Sec. 224 (b)(2) and (c), 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. APPA suggests that such emergency or expedited authority could 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.

FERC's authority to issue rules or orders under Section 224 (b)(1) 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 under sections (b)(2) and (c) are subject to a 90 day sunset in Sec. (d) unless FERC "gives interested persons an opportunity to submit written data, views, or arguments . . ." Unfortunately, there is no requirement for FERC and DOE 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).

Draft Sec. 224(f) does 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. My understanding is that the Critical Infrastructure Information Act processes referenced in Sec. 224 (a)(3) and (f) protect only voluntary disclosures by non-governmental entities to government agencies. As discussed above, a variety of other communications may need additional safeguards. As noted previously, H.R. 2165 contains provisions that deal with these confidentiality concerns in a more comprehensive and effective manner.

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

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