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

HOUSE ENERGY AND AIR QUALITY SUBCOMMITTEE'S

Hearing regarding "Protecting the Electric Grid from Cyber-security Threats"

September 11, 2008

APPA appreciates the opportunity to provide the following testimony for the House Energy and Air Quality Subcommittee's hearing regarding "Protecting the Electric Grid from Cyber-security Threats." I am Susan Kelly, Vice President of Policy Analysis and General Counsel of APPA. With me is Allen Mosher, APPA's Senior Director of Reliability and Policy Analysis.

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.

Introduction

Those of you who follow the electric utility industry closely know how rare it is that its trade associations speak with one voice on a federal energy policy issue. 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 cybersecurity emergencies, however, we have come together. 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 (associations) all support carefully crafted and specific legislation as the basis to deal with the discrete issue of cybersecurity 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 has implemented, with the oversight of the Federal Energy Regulatory Commission (FERC).

I have been asked by the Subcommittee to address the following subjects in my testimony: (a) whether the new federal emergency authority provided in the House discussion draft of legislation would be sufficient, but not excessive; (b) how that authority would fit with the current jurisdictional structure governing the bulk-power system; (c) whether all the governmental and industry actors involved and affected could be expected to respond, if such authority were invoked, in a timely and effective manner; (d) the degree to which the draft represents a consensus of views among stakeholders; (e) the nature of any remaining differences of views on specific provisions of the legislation; (f) the associations' recommended resolutions of those differences; (g) whether there are any important omissions in the draft; and (h) recommendations to the Subcommittee concerning its further actions with regard to this issue and the draft legislation. I will address each of these subjects in turn.

Whether the New Federal Emergency Authority Provided in the Draft Would Be Sufficient, but Not Excessive

The associations support the House discussion draft, **with the specific language options proposed by the associations**. This legislation is intended to fill a narrow gap in the

reliability standards regime that was established under section 215 of the Federal Power Act (FPA). Congress added this section to the FPA in section 1221 of the Energy Policy Act of 2005 (EPAct05). Section 215 was the result of a broad industry consensus in support of mandatory reliability standards. Under section 215, FERC has certified the North American Electric Reliability Corporation (NERC) as the nation's Electric Reliability Organization (ERO). The ERO is charged with the establishment and enforcement of mandatory standards for the bulk-power system intended to maintain its reliability, *i.e.*, to ensure that the lights stay on. NERC develops its reliability standards through a public and transparent standard-setting process that involves literally hundreds of volunteers from various sectors of the electric utility industry. FERC reviews these standards and either approves them or remands them to NERC for further consideration if it finds it cannot approve them. FERC can also order NERC to submit a proposed reliability standard or to revise an existing standard if FERC thinks such a standard is needed to assure reliability of the bulk-power system. NERC and its eight Regional Entities are charged with "front line" enforcement responsibilities for the resulting reliability standards, subject to FERC oversight. FERC also has its own independent standards enforcement authority. NERC's reliability standards apply to utilities in Canada and northern Mexico as well, although the legal and regulatory frameworks differ in those jurisdictions.

APPA believes this industry-based standards development and enforcement framework is working to ensure the reliable planning and operation of the bulk power system. To date, FERC has approved 94 mandatory reliability standards, while at the same time directing the ERO to consider many improvements to these standards. Critical Infrastructure Protection (CIP) is a case in point: so far, NERC has developed and FERC has approved nine CIP

standards. Based on FERC directives, NERC has also initiated a standards development project that will make further improvements to these standards.

Cybersecurity emergencies involving the bulk-power system, however, present a special case, for three reasons. First, cyber security emergencies by their nature entail protection against deliberate malicious attacks intended to disrupt system operations or cause other damaging consequences. In contrast, other reliability standards are generally designed to address random equipment failures, operator errors, and acts of God, such as hurricanes, with which the industry has many years of operational experience. Second, new, unforeseen threats could arise very quickly, leaving little time to react before attacks place reliable bulk-power system operation at risk. The swift pace of changes in information technology increases such risks. While NERC does have expedited standard development procedures in place, and is considering further improvements to those procedures, at present, there is a timeliness issue in such special cases. Third, there is a need for confidentiality regarding the nature of the threat, the risks that it poses to reliable operations, and the measures to be taken to address it, at least until such time as the initial measures can be implemented. NERC is currently considering how its standard-setting process can be revamped to deal with such confidentiality issues, while still getting the industry input needed to ensure that standards are broadly supported and resolve the problem in the most effective manner, without unintended consequences for other aspects of system operations. At this time, however, confidentiality is an issue in such special cases.

For these reasons, the associations support specific legislation that would serve as an appropriate basis to address the unique circumstances that cybersecurity emergencies raise, and no more. Any such legislation should be narrowly drawn to address the identified

problem. In particular, Congress should take care not to undermine the section 215-based reliability standards-setting process. While the regime is still relatively new, it has already brought salutary changes to our industry in the area of reliability. Users, owners and operators of the bulk-power system subject to the regime have made substantial progress in implementing the new reliability standards, including the CIP standards. This mandatory standards regime needs to be allowed to continue to develop and mature.

How the Authority Would Fit with the Current Jurisdictional Structure Governing the Bulk-Power System

The House discussion draft has been crafted to dovetail with the current jurisdictional structure governing the bulk-power system. First, like FPA section 215, its applicability is limited to "users, owners and operators" of the bulk-power system. That term has been defined in section 215(a)(1) as follows:

> The term 'bulk-power system' means—(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.[1]

The practical application of the term "users, owners and operators of the bulk-power system" has been developed in the course of NERC's implementation of the mandatory reliability standards I previously discussed. NERC has a Compliance Registry that lists those users, owners and operators of the bulk-power system that must comply with at least some portion of NERC's reliability standards. Those listed in the Compliance Registry are included based on Compliance Registry Criteria that have been developed by industry stakeholders and NERC, and subsequently approved by FERC. Retail customers and local distribution

[1] Note also that FPA section 215(k) provides that "[t]he provisions of this section do not apply to Alaska or Hawaii."

facilities, small generators, and small utilities are generally excluded from this reliability regime.

In the view of the electric utility industry and its State regulators, it is best to limit the new cybersecurity legislation to this same universe of facilities and entities. To do otherwise (for example, to expand the reach of the legislation to encompass local distribution facilities) would raise jurisdictional and implementation issues that could greatly complicate consideration of legislation on this issue. As members of the Subcommittee are well aware, local distribution facilities in the States are regulated by State regulatory commissions, which are responsible for ensuring that retail utility service is provided safely and reliably within their respective jurisdictions. As Congress recognized in FPA section 215(i)(3), the authority of the States to regulate the reliability of local distribution networks and service should be preserved, with FERC's regulatory authority focused on the operations of the bulk-power system.

For these reasons, the industry believes that the jurisdictional lines drawn in the House discussion draft are the proper ones.

Whether the Governmental and Industry Actors Involved and Affected Could Be Expected to Respond, if Such Authority Were Invoked, in a Timely and Effective Manner

The House discussion draft has been fashioned to allow FERC to address cybersecurity emergencies as swiftly as possible, while still providing for appropriate consultation with governmental authorities (including Canadian and Mexican authorities) and affected users, owners and operators of the bulk-power system in the United States. The industry itself is proceeding up the learning curve on responding to notices of cybersecurity threats, having

learned a number of lessons through its response to the Aurora vulnerability in 2007. Since I am not an expert in this area, I will defer on this issue to the other industry witnesses appearing before the Subcommittee.

The Degree to Which the House Discussion Draft Represents a Consensus of Views Among Stakeholders

As I noted at the outset of my testimony, APPA and the other associations support carefully crafted legislation to address cybersecurity emergencies. While individual associations may have differed over certain specifics of the proposed legislation at the outset, intense negotiations among the associations themselves and jointly with FERC over the last several weeks have resulted in a consensus association position on legislation.

The Nature of Any Remaining Differences of Views on Specific Provisions of the Legislation and Your Recommended Resolutions of those Differences

The associations negotiated at length with representatives of FERC regarding the earlier version of the House discussion draft. We were able to reach closure on many issues, and we thank the FERC staff for the constructive and positive attitude it maintained during these negotiations. Nonetheless, we were unable to reach closure on three issues, as reflected in the recently released version of the House discussion draft. These three areas are:

- Definition of "Cyber security Threat." The industry and FERC agreed on most elements of this definition, but differ in two respects. First, we believe that there should be a *substantial* likelihood of a malicious act for the federal government to conclude that there is a cybersecurity threat that would trigger the need for

emergency action. FERC would prefer a simple "likelihood" of such an act. Second, we believe there should be both a substantial likelihood of a malicious act *and* a substantial possibility of disruption to the operation of the system in the event of such an act, to constitute a "cybersecurity threat." FERC would prefer the definition to be phrased in the disjunctive ("or"). The associations believe their preferred definition limits the legislation appropriately to cybersecurity emergencies – meaning threats that have a substantial likelihood of happening and that could substantially disrupt the reliable operation of the bulk-power system if they do happen.

- Inclusion of "Other National Security Threats." FERC would prefer to expand the legislation to include "other national security threats" in addition to cybersecurity threats. The associations believe that other government entities, both state and federal, have more direct responsibilities in the general area of national security. Moreover, this additional authority is quite vague in its wording and hence potentially all-encompassing in nature, which in and of itself raises substantial concerns. Finally, including such language could spark an intense discussion that could slow down the legislation considerably. For all these reasons, the associations do not favor including it.

- "Sunset" of Interim Measures that FERC Enacts under Subsection (b). The industry and FERC negotiated at length regarding the "sunset" provision of subsection (d) (entitled "Discontinuance"). We were able to reach closure on almost all of the issues, but one remains outstanding. The associations believe that the sunset provision in subsection (d)(4) should apply to both interim measures FERC implements under subsection (b) and emergency measures it implements under

subsection (c). We believe this should be the case because we regard measures and orders under both sections as either being limited in time by their nature, or to be replaced by reliability standards NERC develops using section 215 procedures. FERC, however, does not accede to this position as to actions it takes under subsection (b).

While the associations could not reach closure with FERC on these three issues, this should not overshadow the substantial progress we did make in the negotiations regarding draft legislation. For all of our associations and the federal regulator to reach closure on the issues this legislation raises, save these three, is noteworthy.

Whether there Are Any Important Omissions in the Draft

The associations generally believe that the House discussion draft, with acceptance of the associations' proposed language options, would cover the important areas that need to be covered. For the reasons stated above, others (and, in particular, FERC) may disagree with the associations' view on this issue.

Recommendations to the Subcommittee Concerning Its Further Actions with Regard to This Issue and the Draft Legislation

The associations support narrowly focused legislation as a basis to address the issue of cybersecurity emergencies involving the bulk-power system. We strongly urge Congress to retain the carefully crafted legislative language reflected in the House discussion draft, with the proposed language options that the associations support, as the process moves forward.

Conclusion

Thank you for the opportunity to present APPA's views on the House discussion draft. We look forward to continuing to work with the Subcommittee on this important issue and are available to provide any further assistance.