



Jonathan P. Trotta
202.728.3035 DIRECT
202.572.9956 DIRECT FAX
jtrotta@stinson.com

September 23, 2010

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Notice of Comment, National Broadband Plan Recommendation to Create a Cybersecurity Roadmap, PS Docket No. 10-146; GN Docket No. 09-51

Dear Ms. Dortch:

Enclosed on behalf of the Edison Electric Institute ("EEI"), American Public Power Association ("APPA"), National Rural Electric Cooperative Association ("NRECA") and the Utilities Telecom Council ("UTC") are comments in the above-referenced proceeding.

These comments are being filed electronically using the Commission's Electronic Comment Filing System ("ECFS") for inclusion in the record of the above-referenced proceeding.

Respectfully submitted,

STINSON MORRISON HECKER LLP

A handwritten signature in black ink, appearing to read "Jonathan P. Trotta", is written over a printed name and title.

Jonathan P. Trotta
Counsel to Edison Electric Institute

Attachment

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	PS Docket No. 10-146
)	
National Broadband Plan)	GN Docket No. 09-51
Recommendation To Create A)	
Cybersecurity Roadmap)	

**JOINT COMMENTS OF THE EDISON ELECTRIC INSTITUTE, AMERICAN
PUBLIC POWER ASSOCIATION, NATIONAL RURAL ELECTRIC
COOPERATIVE ASSOCIATION AND THE UTILITIES TELECOM COUNCIL**

The Edison Electric Institute ("EEI"), American Public Power Association ("APPA"), National Rural Electric Cooperative Association ("NRECA"), and the Utilities Telecom Council ("UTC") (collectively the "Associations") on behalf of their member electric utilities, hereby submit the following comments in the above-referenced proceedings in response to the Federal Communications Commission's ("FCC" or "Commission") request for comments on the creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and to develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks in coordination with federal partners.¹

EEI is an association of United States investor-owned electric utilities and industry associates worldwide. Its U.S. members serve almost 95 percent of all customers served by the shareholder-owned segment of the U.S. industry, about 70 percent of all electricity customers, and generate about 70 percent of the electricity

¹ See FCC Notice of Comment, NBP Recommendation to Create a Cybersecurity Roadmap, PS Docket No. 10-146; GN Docket No. 09-51 (August 9, 2010) ("Notice").

delivered in the U.S. EEI frequently represents its U.S. members before federal agencies, courts and Congress in matters of common concern, and has filed comments before the Commission in various proceedings affecting the interests of its members.

NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to approximately 42 million consumers in 47 states or 12 percent of the nation's population. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA's members are not-for-profit, consumer-owned cooperatives, formed to provide reliable electric service to their owner-members at the lowest reasonable cost.

APPA is the national service organization representing the interests of the over 2,000 publicly-owned, not-for-profit electric utilities. Currently, over 70 percent of APPA's members serve communities with less than 10,000 residents, and approximately 45 million Americans receive their electricity from public power systems operated by municipalities, counties, authorities, states, or public utility districts. Approximately 300 of those systems operate external communications services with over 1,000 providing their own internal services.

UTC is the international trade association for the telecommunications and information technology interests of electric, gas and water utilities and other critical infrastructure industries, including pipeline companies. Its members include investor-owned, municipal and cooperatively organized utilities.

The Associations' members may be directly and indirectly affected by the instant proceeding, as users of broadband communications networks and services. The primary

interest of the Associations' members in this proceeding is the advancement of policies that promote development of secure communications infrastructure to support the safe, reliable and efficient delivery of essential utility services to the public at large.

COMMENTS

In order to provide safe, reliable electric service, utilities must have communications systems that are both reliable and secure. Electric utilities provide critical services that are relied upon by most, if not virtually all, of this country's residential and business consumers, and the national interest requires that utility networks must remain protected and secure. Electric utilities are among the nation's largest users of communications services, and rely on both commercial and private communications systems for the safe and reliable delivery of power to consumers at reasonable costs. Secure communications networks are essential to utility operations, and demands on utility communications systems will increase with the deployment of Smart Grid technologies and other broadband applications. This increased demand will present new and complicated cybersecurity issues that must be planned for in order to ensure the delivery of safe and reliable electric service, to safeguard the rights of utility customers, and to maintain a culture of trust between electric utilities and their customers and their personal information. Accordingly, the Commission, in considering the actions it should take to identify and address critical cybersecurity threats to communications infrastructure and end users, should take into account the needs and concerns of electric utilities as set forth herein.

A. A Cybersecurity Roadmap Must Support Smart Grid and Existing Private Communications Networks

It is critical that any Cybersecurity Roadmap developed by the Commission support electric utilities' Smart Grid efforts, as well as private communications networks relied on by utilities to carry out their core mission of safely and reliably delivering power to consumers at reasonable costs. Utility infrastructure, including the communications networks used to manage and monitor that infrastructure, is undoubtedly "critical infrastructure," the adequate protection of which is essential to our economic health, public safety and national security. Indeed, without adequate and durable utility service, public and commercial communications networks cannot function.

Electric utilities and critical infrastructure industries rely on both commercial communications systems and private internal broadband networks to provide levels of reliability, security and coverage necessary to meet utility communications needs. Utilities rely heavily on wireline and wireless communications to support maintenance, remote control and monitoring, dispatch of field crews in service territories, and communication with customer meters. Utilities also rely on different broadband applications to support their internal critical operations needs, including mapping for remote locations and for pinpointing outages or other problems, the ability to transmit schematics, blueprints and other necessary data to field crews, as well as video surveillance to prevent copper theft and to provide overall security throughout the grid. Similarly, utilities depend on radio networks for internal communications between offices, to improve operational efficiency and to quickly and effectively respond to weather events.

Much of this information is sensitive in nature and must be securely communicated over utilities' existing private networks in addition to any commercial

networks on which utilities might rely. Utilities invest heavily in cybersecurity for all of their electric, business and communications systems, including protection of customer information. Public power, cooperative and investor-owned utilities frequently collaborate to ensure they are implementing effective cybersecurity procedures and technology. It is important, then, for the Commission not to lose sight of utilities' existing cybersecurity efforts and need for a secure communications network that includes both public and private structures. An efficient grid requires utilities to rely, not only on commercial networks, but also on private communications systems for safe and reliable operations, and any Cybersecurity Roadmap or other cybersecurity actions taken by the Commission should support utilities' use of private communications networks.

In addition, new and expanding Smart Grid data needs and the deployment of additional broadband applications will require increased security as utilities come to manage data from large numbers of distributed generation energy resources and automation devices across the grid. Therefore, future cybersecurity directives must bear in mind the implications of the Smart Grid, and the FCC must work to develop a Roadmap that supports Smart Grid development and utilities' efforts to implement Smart Grid technologies. If suitable cybersecurity features for utility Smart Grid networks are not implemented, the goals of Smart Grid and the National Broadband Plan may be compromised.

B. FCC Should Coordinate Cybersecurity Efforts with other Federal Agencies

As the Commission moves forward with its Cybersecurity Roadmap, it should be mindful of the efforts of other federal agencies in this arena. Cybersecurity is a broad subject area, with implications across multiple fields and industries. The Commission,

then, should coordinate its activities in this area with other federal agencies and departments such as the Department of Homeland Security's National Security Telecommunications Advisory Committee ("NSTAC"), the Federal Energy Regulatory Commission ("FERC"), the National Institute of Standards and Technology ("NIST") and the Department of Energy ("DOE"), all of which have engaged in cybersecurity research, and have developed approaches to address various cybersecurity issues. Too often the electric utility industry is left out of these important conversations at organizations such as NSTAC. It is imperative to include electric utilities in all of these discussions if the optimal approach to addressing cybersecurity across sectors is to be achieved.

A Cybersecurity Roadmap should be in harmony with these efforts, and the Commission should ensure that its activities do not duplicate or conflict with other cybersecurity efforts being made within the federal government.

The FCC would surely benefit from closely considering the initiatives and progress being made elsewhere regarding research and development of cybersecurity issues and related solutions, and the Associations urge the Commission to review the cybersecurity threats to communications networks or users identified by other departments and any programs or guidance adopted by other agencies to address these threats.

C. National and International Cybersecurity Standards Exist and Should Be Recognized in the Cybersecurity Roadmap

The development and implementation of new secure protocols, including payloads and communications protocols, for communications infrastructure and end users, and for other critical infrastructure are subject to national and international

standards. The North American Electric Reliability Corporation (“NERC”) is certified by FERC as the Electric Reliability Organization (“ERO”) responsible for the developing and enforcing reliability standards for the North American bulk power system. NERC’s standards include Critical Infrastructure Protection (“CIP”) reliability standards that provide the framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system and require regulated entities to define methods, processes, and procedures for securing those systems.

The Institute of Electrical and Electronics Engineers (“IEEE”), for instance, is responsible for the development and integration of interoperability standards for industries worldwide. As part of this process, IEEE has engaged in development of standards to help electric utilities retrofit their communications systems to protect against cyber attack, and to protect utility communication installations from lightning. IEEE develops consensus standards such as these through an open process that engages all areas of industry.

The Commission, then, should acknowledge the considerable work being done in the area of cybersecurity standard development on a national and international level, and should proceed carefully with its Cybersecurity Roadmap to ensure that its efforts to identify cybersecurity threats to communications infrastructure and end-users, and to develop solutions, do not overreach the scope of its expertise.

D. APPA, EEI, NRECA and UTC Support Electric Utility Involvement on Communications Matters Including Cybersecurity

Finally, as the Commission proceeds with its Cybersecurity Roadmap and related efforts, the Associations support opportunities for continued involvement by electric

utilities on communications matters, including cybersecurity for telecommunications carriers.

CONCLUSION

WHEREFORE, for the foregoing reasons, the Associations respectfully request that the Commission consider these comments and ensure that Commission action ordered regarding the creation and implementation of a Cybersecurity Roadmap is consistent with them.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ David K. Owens

David K. Owens
Executive Vice President

Aryeh B. Fishman
Director, Regulatory Legal Affairs
Office of the General Counsel

Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
(202) 508-5000
afishman@eei.org

H. Russell Frisby, Jr.
Jonathan P. Trotta
Counsel
STINSON MORRISON HECKER LLP
1150 18th Street, NW, Suite 800
Washington D.C. 20036-3816
(202) 785-9100
(202) 785-9163 (Fax)
rfrisby@stinson.com
jtrotta@stinson.com

Dated: September 23, 2010

NATIONAL RURAL ELECTRIC COOPERATIVE
ASSOCIATION

/s/ David Predmore

David Predmore
Corporate Counsel

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203

(703) 907 – 5500
david.predmore@nreca.coop

AMERICAN PUBLIC POWER
ASSOCIATION

/s/ Corry Marshall
Government Relations
Representative

American Public Power Association
1875 Connecticut Ave, N.W.
Suite 1200
Washington, D.C. 20009
(202) 467-2975
cmarshall@appanet.org

UTILITIES TELECOM COUNCIL

/s/ Mike Oldak
Mike Oldak
Vice President & General Counsel

Brett Kilbourne
Director of Regulatory Services &
Associate Counsel

Utilities Telecom Council
1901 Pennsylvania Avenue, NW
Fifth Floor
Washington, DC 20006
(202) 872-0030
brett.kilbourne@utc.org