American
Public Power
Association

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

Ph: 202.467.2900
Fax: 202.467.2910
www.PublicPower.org

April 29, 2013

(Via cyberincentives@ntia.doc.gov)

Mr. Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, D.C. 20230

Dear Mr. Lee:

The American Public Power Association (APPA) appreciates the opportunity to comment on incentives that could allow for robust private sector engagement in the development and adoption of a national Cybersecurity Framework. This Framework's importance cannot be overstated, especially when combined with the many ongoing cybersecurity activities already being undertaken by the electric utility sector. Bringing other private sector entities into similar frameworks to that of the electric sector and incentivizing cross-sector cybersecurity practices is a step APPA applauds and looks forward to participating in.

APPA is the national service organization representing the interests of not-for-profit, state, municipal and other locally-owned electric utilities throughout the United States. More than 2,000 public power systems provide over 15 percent of all kilowatt-hour ("kWh") sales to ultimate customers, and do business in every state except Hawaii. APPA utility member's primary goal is providing customers in the communities they serve with reliable electric power and energy at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of APPA-member electric utilities with the long-term interests of the residents and businesses in their communities. Collectively, public power systems serve over 47 million people.

APPA urges the Department of Commerce to take as a starting point our firm view that each of APPA's members is committed to ensuring the cybersecurity of our systems and will take reasonable steps to adopt voluntary standards, policies and best practices that ensure cybersecurity at reasonable costs without other unintended consequences. Thus, APPA suggests that the Department should focus less on creating financial or other incentives for the adoption of the Cybersecurity Framework, but rather toward removing barriers to full participation in the Administration's cybersecurity programs initiated pursuant to the President's Executive Order on Cybersecurity, ensuring the effectiveness of the overall Framework to address electric sector needs, and addressing the specific resource limitations and training needs of small public power entities.

First, electric utilities that own and operate the bulk power system are already subject to mandatory and enforceable cybersecurity standards established after passage of the Energy Policy Act of 2005. EPAct requires electric utilities to comply with reliability and cybersecurity standards developed by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission. In marked contrast, the EO contemplates the development of a voluntary cybersecurity standards framework applicable to all critical infrastructure sectors in the United States. A clear separation between the voluntary EO Framework and mandatory standards applicable to the electric

sector must be maintained. Any implication that the NIST Cybersecurity Framework might be used to establish a new baseline for mandatory NERC standards must be avoided.

Second, APPA believes sector-specific agencies can do much to encourage broad adoption and application of the final Cybersecurity Framework by following the same approach as the Department of Energy adopted with its Electricity Sector Cybersecurity Capability Maturity Model of working with the electric sector trade associations to educate them on the ESC2M2 and provide guidance in the field on how it can be applied successfully to each utility's unique circumstances.

Third, APPA cannot overemphasize the importance of timely information sharing with the private sector through the Electric Sector Information Sharing and Analysis Center and through other forums. We are, however, concerned that the EO appears to contemplate funneling information provided by the federal government through private sector information security providers. Allowing electric utilities unconstrained access to the Enhanced Cyber Security Services program without a need for a pay to play system would be more likely to ensure broad electric sector participation. We also see substantial benefits from an increased number of security clearances.

Finally, liability protections for electric utilities that report cyber threat information must be explored. This could possibly be a useful tool to incentivize participation, but it should be studied first so the benefits and drawbacks can be fully understood.

Thank you for the opportunity to submit these comments. Should you have any questions, please do not hesitate to contact us.

Respectfully yours,

/S/

Allen Mosher
Vice President of Policy Analysis and Reliability Standards
Nathan Mitchell
Director, Electric Reliability Standards and Compliance
1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009
(202) 467-2944
amosher@publicpower.org
nmitchell@publicpower.org