(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 Electric Power Supply Association (EPSA) appreciates the opportunity to comment on incentives and other public policy recommendations associated with the National Institute of Standards and Technology's March 28, 2013 Notice of Inquiry. EPSA appreciates NIST's willingness to collect input regarding industry participation in the Cybersecurity Framework and ensuring infrastructure security. Attached are EPSA's comments.

Comments of the Electric Power Supply Association -- April 29, 2013

On the National Institute of Standards and Technology (NIST) March 28, 2013 Notice of Inquiry (NOI)

INCENTIVES TO ADOPT IMPROVED CYBER SECURITY PRACTICES

EPSA[1] is the national trade association representing competitive power suppliers, including generators and marketers. Competitive suppliers, which collectively account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities. EPSA seeks to bring the benefits of competition to all power customers. EPSA is part of broad coalition of electric power stakeholders focused on cyber security who provided comments on the NIST Request for Information ("RFI") published in the Federal Register on February 26, 2013. The coalition consists of trade associations representing the full range of electric system infrastructure and customers in North America.

Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the competitive power suppliers' top priority. Competitive power suppliers take cyber security threats very seriously. EPSA shares the goals of Executive Order 13636: to enhance the security of the Nation's critical infrastructure through public-private partnerships and encourage participation in the Critical Infrastructure Cyber security Program ("the Program"). We therefore welcome the opportunity to provide input to NIST and the Department of Commerce on efforts to promote voluntary adoption of the Cyber security Framework.

The power grid is a complex infrastructure made up of networked generation, transmission, distribution, control, and communication technologies, which can be damaged by natural events such as severe storms, as well as malicious events such as a cyber- attack. Cyber security is not new to the electricity sub-sector as it has become a priority over the past decade. As threats have become more sophisticated, the sector continues to strengthen its defenses.

As a result of passage of the Energy Policy Act of 2005, the electricity sub-sector is subject to mandatory, enforceable cyber security standards under the jurisdiction of the Federal Energy Regulatory Commission ("FERC"). The standards drafting process, which is conducted by the North American Electric Reliability Corporation ("NERC"), relies heavily on the technical expertise of industry experts and are approved by federal

[1] **The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.**

regulators to ensure that cyber security standards are technically and operationally sound and do not result in unintended consequences.

Cyber threats require quick action and flexibility, which makes timely dissemination of threat information and analysis critical to ensuring appropriate information sharing when protective actions need to be taken. Therefore, EPSA strongly supports the provisions of the Executive Order furthering timely information sharing about cyber threats among the government and owners and operators of critical infrastructure, including generation owners.

Close collaboration between government and industry is needed to truly mitigate cyber risk. Just as our industry does not have intelligence gathering capabilities, the government does not have experience with operating an electric utility system. Both industry and government have roles to play, which require a cooperative working relationship. Our efforts will be vastly improved with better information sharing and a clearer understanding of roles among various government agencies, which the Executive Order seeks to achieve.

As part of an electric industry coalition, EPSA commented on the February 26, 2013 NIST RFI and strongly supported the Executive Order's directive that the Cyber security Framework "shall provide a prioritized, flexible, repeatable, and performance-based and cost- effective approach." EPSA and the other electric industry groups asserted that the framework must:

(1) Be high-level and flexible, to ensure that the Cyber security Framework can be adapted to the Nation's diverse critical infrastructure sectors, without unintended consequences;

(2) Build upon each sector's existing processes, standards and guidance, including the sector-specific regulatory standards which already exist in the electric and nuclear industries;

(3) Avoid time-consuming and unnecessary duplication of efforts;

(4) Preserve and build upon existing public-private partnerships; and

(5) Be risk-based and cost-effective.

The March 22 Notice of Inquiry ("NOI") recognizes that in order to encourage participation in the Cyber Security Framework Program further incentives may be necessary to encourage sufficient private sector participation in the Program. EPSA does not specifically believe "incentives" are required, however all electric industry entities deserve an equal opportunity to recover costs associated with security issues

related to cyber security threats. Therefore, EPSA's position is that the framework must be risk-based and cost effective.

Prior to the issuance of Executive Order, both the Congress and the Administration have been looking at potential legislative action on cyber security and protecting the nation's Bulk Power System ("BPS") from cyber-related attacks. EPSA, along with several other electricity trade associations, has been supportive of cyber security legislation that protects the nation's BPS.

Any cyber security legislation should fall under FPA Section 215 so that it will apply to "owners, users or operators" of the BPS. Legislation should also be limited to cyber security threats only, and provide for a "sunset" of any FERC emergency order. Additionally, legislation or executive order/action should ensure that all owners and operators of the BPS have a fair and realistic opportunity to recover incurred costs for protecting the grid from cyber-attacks or taking emergency action in response to imminent threats.

Cost-Benefit Impact

The issue of cost-benefit impact on cyber security mitigation has been flagged by both the Center for Strategic and International Studies' ("CSIS") Commission on Cyber Security for the 44th Presidency and the Government Accountability Office's ("GAO") National Cyber Security Strategy. These reports encourage the government to provide owners and operators of energy assets a value proposition and provide private sector incentives much like NIST is exploring in the NOI. Additionally, the CSIS and GAO reports urged the use of cost-benefit analyses to ensure the efficient use of cyber security resources. In line with the GAO and CSIS findings, federal regulators need to implement a cyber security strategy that is cost efficient and fair. It is important that the entity directing emergency actions for protection of the BPS understand both the benefits and costs of such actions.

For instance, the uncertainty of costs associated with cyber security could pose a barrier to long-term power purchasing contracts, as neither the buyer nor the seller wants exposure to unknown costs. Additionally, through established rules and structures governing wholesale electricity markets, competitive suppliers may not be able to pass through costs that address cyber security threats. Furthermore, competitive power suppliers cannot seek cost recovery from State Public Service Commissions for complying with mandated cyber security orders. Having an established regulatory mechanism in place that allows for the recovery of cyber-related costs will alleviate these concerns.

An Appropriate Cost Recovery Mechanism

As described above, a mechanism for cyber-related costs is necessary so that all private sector entities will be able to recover cyber related costs on an equal basis. Directives from the federal government to protect the nation's electricity grid from a cyber attack, or to implement emergency orders for national security purposes, is beyond the scope of normal business operations. An uneven playing field would exist if others in the power sector were allowed to have their costs recovered, but competitive suppliers were not. Thus, it is imperative that upon implementation of emergency cyber security measures, NIST and other relevant federal regulators ensure that there is sufficient cost recovery for all industry infrastructure owners to ensure grid security. EPSA believes that determining how to allow for prudent recovery of costs is well within the scope of FERC's expertise and authority.

Proposed Solution

A reasonable approach to solving this concern and ensuring reliable non-discriminatory wholesale electric service is to include language that directs FERC to develop a cost recovery mechanism, which would allow companies to go before the Commission to recover prudently incurred costs as a result of complying with federal cyber security mandates.

Precedent

There are past examples of FERC taking such action in emergency cases. In particular, FERC issued a policy statement after the September 11, 2001 terrorist attacks, which implemented a cost recovery mechanism for compliance with the emergency orders that were established at that time. Similarly, in this instance, FERC would have the flexibility to decide the most feasible manner for an appropriate cost recovery mechanism for cyber-related costs on either a generic or a case-by-case basis.

Conclusion

In closing, we are pleased that NIST recognizes the need for the private sector to be given the appropriate signals by Government so that cyber security risks can be addressed on a voluntary basis by all private sector entities on an equitable basis. Competitive power suppliers should not be disadvantaged because they cannot pass through these costs. Instead, allowing competitive suppliers -- or any "owner, user or operator" of the BPS -- to go before FERC to seek the recovery of costs prudently incurred in response to a directive by the federal government in a cyber emergency, is a sensible policy solution. Such an option would place all electricity providers on equal footing as we all do our part to secure and protect the reliability of the nation's electricity grid.

Sincerely,

William S. Burlew

Vice President, Government Affairs