701 Pennsylvania Avenue, N.W. | Washington, D.C. 20004-2696 | www.eei.org
202.508.5615 | Fax: 202.508.5673 | Mobile: 202.258.2909 | ecomer@eei.org

Power by Association℠

Edison Electric Institute

Edward H. Comer
Vice President, General Counsel
& Corporate Secretary

April 29, 2013

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 Edison Electric Institute (EEI) appreciates the opportunity to comment on incentives and other public policy recommendations that will lead to robust private sector engagement in the Cybersecurity Framework and a strong government-industry partnership in defense of critical infrastructure.

EEI is the trade association of U.S. shareholder-owned electric companies. Its U.S. members serve more than 98% of the ultimate customers of electricity in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. EEI is part of a broad coalition of electric power stakeholders focused on cybersecurity. This cybersecurity coalition includes several major trade associations representing the full range of electric generation, transmission and distribution companies in the United States, as well as regulators, Canadian interests and large industrial customers.

I. The Electric Sector Perspective

Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the electric utility industry's top priority. Thus, our industry takes cybersecurity threats very seriously. EEI shares the goals of Executive Order 13636 to enhance the protection and resilience of the Nation's critical infrastructure through public-private partnerships.

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. Cybersecurity is not new to the electricity sub-sector—it has been a growing priority over the past decade. The sector employs threat mitigation actions focused on preparation, prevention, resiliency, response, and recovery in its operations. As threats to the grid continue to grow 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 has been subject to mandatory and enforceable cybersecurity standards under the jurisdiction of 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 working in conjunction with federal regulators to ensure that cybersecurity standards are technically and operationally sound and do not result in unintended consequences. Considerable resources and much time have been dedicated to the drafting and implementation of these cybersecurity standards.

Owners and operators of nuclear energy facilities are also subject to extensive regulation by the Nuclear Regulatory Commission (NRC) to ensure cyber protection. The nuclear energy industry implemented a cybersecurity program in 2002 to protect critical digital assets. In 2009, the NRC built upon this program by establishing cybersecurity regulations for U.S. nuclear reactors. A memorandum of understanding and policy statement by the NRC ensure that there is good coordination between NERC and the NRC, so that no gaps in protection exist for nuclear generators.

EEI, our members and others in the electric industry also work with government partners in a variety of voluntary contexts to protect against cyber threats. Through these efforts, we have learned that standards enforce good business practices and encourage a baseline level of security, but standards alone are not sufficient because the cybersecurity threat environment is constantly changing and threats and our nation's adversaries evolve rapidly.

Imminent cyber threats require quick action and flexibility. Timely dissemination of threat information and analysis must play an important role in informing protective actions. Therefore, EEI 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.

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 the expertise to operate an electric utility system. Close collaboration with the government is also needed to practice emergency response protocols before a disaster strikes. Both industry and government have roles to play, which require a close working relationship. Our efforts will be vastly improved with better information sharing ability and a clearer understanding of roles among various government agencies, which the Executive Order seeks to achieve.

EEI also agrees with the Executive Order that a Cybersecurity Framework "shall provide a prioritized, flexible, repeatable, and performance-based, and cost-effective approach." To that end, we believe that the framework must:

1. Be high-level and flexible, to ensure that the Cybersecurity 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 sector-specific regulatory standards which already exist in the electric and nuclear industries;

3. Avoid duplication of effort and streamline the flow of information to ensure the right people have access to the right information in a timely manner;

4. Preserve and build upon existing public-private partnerships; and

5. Be risk-based and cost-effective.

II. Incentives Should Apply to the Entire Private Sector; Not Just Those Who Would Otherwise Not Participate

Our industry believes that policy changes are needed to incent and improve the private sector's readiness, and to eliminate policy barriers that can hinder good cybersecurity practices. These are described below. However, as an initial matter we stress that these measures are not simply needed to encourage voluntary participation in a cyber program. Rather, they are necessary and appropriate because they will help improve the cybersecurity posture of the private sector.

EEI's members are taking extraordinary efforts to protect their systems and work with government and industry partners. They are doing so in the absence of incentives because of their obligation to protect the critical infrastructure they own and operate. New policy incentives should support these efforts by creating opportunities to share information, collaborate with the government, as well as allowing for flexibility in approaches and liability protections to ensure lawsuits do not loom over those who have acted in good faith.

The remainder of our comments will highlight the most important incentives for our industry and indicate which will require legislation to implement.

III. Cybersecurity Policy must Promote Flexibility and Adaptability, rather than Detailed Rigid Standards

Our experience with standards development and specifically with the development of cyber standards convinces us that the cyber Framework by the National Institute of Standards and Technology (NIST) must build upon existing practices and be flexible and adaptable to constantly evolving technologies, threats, and circumstances. Any attempt by NIST to develop new standards for industry sectors should be avoided.

IV. Collaboration, Information Sharing and Access to New Technologies require certain protections, including protection from Disclosure of Sensitive Information

We strongly support the information-sharing provisions of the Executive Order and believe we need appropriate legislation to simplify and expedite information sharing between industry and the government and among different industry sectors.

Legislation is necessary to enable businesses to participate in certain information sharing in order to provide legal certainty to businesses that share information with the government and with each other. This includes provisions to assure that information which businesses voluntarily provide to the government is not disclosed publicly or otherwise used in a regulatory or enforcement context. Businesses may also need limited antitrust protection in order to share information and best practices with each other.

Conversely, when the government provides confidential information to business, we need legal assurances that we will not be required to disclose such information in a way that compromises that information. For example, if SEC investor disclosure requirements are applied so as to require a business to advise its investors whenever a government agency provides a warning to a sector or specific business, such disclosure may compromise the government's information gathering mechanisms and inhibit the sharing of information. We understand that warnings are likely to be fragmentary and vague - i.e., mentioning an unknown type of attack, at an unknown time and of unknown intensity. It should be sufficient for investor disclosure purposes if a business has generally disclosed the possibility of such events and their impacts in annual 10-K statement. However, if a business is also required to provide notices when it receives other warnings, and particularly warnings that it may be a specific target, there will be a disincentive to the government to share this information. The SEC situation may be only one example of where government notice requirements may conflict with good cyber defense policy. Comparable issues may arise in an economic regulatory context.

We urge the Department of Commerce to undertake a careful consideration of these types of notice issues in coordination with the SEC and other federal and state regulatory agencies to determine how we can best protect sensitive information in light of other policy goals.

V. Cybersecurity Measures must be Cost Effective and Justifiable to Economic Regulators

One of the most important ways to incent business participation in assuring cybersecurity is to promote cost-effective cyber practices and, as we indicated above, avoid approaches that are unnecessarily complex and costly. The electric sector is unique among business in that we must justify the need for, prudence and cost effectiveness of expenditures for cybersecurity to economic regulators at the state and federal level in order to be able to recover such costs in rates to our customers. Thus, our regulators and customers would benefit from government efforts to explain in a secure, public manner the types of cybersecurity approaches that are needed, prudent and cost-effective.

In addition, government agencies which have access to good cyber tools and practices and which are initiating projects to develop even better tools and practices will incent private sector participation by sharing quickly the benefits of their knowledge with their partners in the private sector.

Finally, as we indicated in our comments on the NIST Framework, individual companies do not have the resources to assess the supply chain integrity of every component – from millions of lines of software code to thousands of hardware components. Companies are working with each other, the Federal government, and vendors to reduce the supply chain risk through a number of security efforts including: adoption of secure coding practices, application and component testing, improved procurement language, use of supplier monitoring tools and best practices, and analysis of software and hardware. If normal standard-setting approaches lead to lengthy delays in accomplishing this, however, it may be necessary to expedite the process by enabling some of these measures to proceed without anti- trust concerns.

VI. The National Security Aspect of Cybersecurity Requires a Different Approach to Liability

EEI believes legislation is needed to remove legal uncertainties and barriers to expanded cyber protection. As indicated above, information shared with the government should be provided safe harbor from the risk of costly litigation, be exempt from public disclosure and be kept confidential from regulatory and enforcement agencies.

Business also needs protections to be able to share information with other businesses and the government without risk of lawsuits, public disclosure, regulation and antitrust concerns.

Normal liability standards simply do not apply in cyber events, particularly for critical infrastructure that is deliberately targeted for national security purposes. Legislation is needed to extend liability protections and avoid costly, complicated and distracting litigation which could threaten to disclose important information about cyber defenses.

VII. Conclusion

EEI appreciates the opportunity to express our views about the governmental policies which can incent or hinder effective cybersecurity protection within the private sector. We look forward to continuing our government-industry partnership to achieve greater cybersecurity protections. Please contact Mr. Scott Aaronson at 202-508-5481, saaronson@eei.org if you have any follow-up questions about our comments.

Sincerely,

Edward H. Comer
Vice President, General Counsel
& Corporate Secretary