



September 27, 2012

The Honorable John D. Rockefeller IV
Chairman
Senate Committee on Commerce, Science, and Transportation
254 Russell Senate Office Building
Washington, DC 20510-6125

Dear Chairman Rockefeller:

As a coalition representing every segment of the electric utility and nuclear power industries, we write today in reference to the letter you sent Fortune 500 companies regarding cyber security legislation. While your letter reached 24 electric utility companies, we write on behalf of all the owners, users, and operators of the electric grid we collectively represent, and that have a role in securing the grid.

We share your goal of protecting the nation's critical infrastructure from cyber threats. After several months of working with the various committees drafting legislation, we, too, were hopeful Congress could reach agreement on a bill to foster coordination between the federal government and private sector and improve the nation's ability to prepare for—and respond to—the array of cyber threats we face.

It is noteworthy that so many electric sector stakeholders have banded together to work on cyber security issues despite disparate membership and occasionally competing policy goals. In fact, given that the bulk electric grid is highly integrated, but with multiple owners, users, and operators, we have found common cause to work together to secure and protect this critical infrastructure.

In addition to close collaboration as an industry, we also are working directly with government partners to more thoroughly understand the threat environment and, thus, better protect our systems. We agree completely that an innovative and cooperative approach between the private sector and federal government is imperative, and our members already are committing their expertise and leadership to keep the bulk electric grid as secure and resilient as possible.

For example, following recommendations in an October 2010 report to the President by the National Infrastructure Advisory Council (NIAC), the electric power industry proactively contacted the Obama Administration and has been working to improve coordination with the government at the most senior levels. Under the auspices of the NIAC report, several CEOs met with White House National Security Staff, Department of Energy (DOE) Secretary Steven Chu, and Department of Homeland Security (DHS) Secretary Janet Napolitano on July 23. This meeting has resulted in a more robust collaboration between the public and private sectors, including a more recent classified briefing for senior industry executives and the promise of an ongoing dialogue and direct working relationship between industry and government leaders. Further, there is the Electricity Sector Cybersecurity Capability and Maturity Model that DOE and DHS have undertaken in partnership with the private sector and public policy experts to gauge industry readiness and provide guidance for policymaking. Beyond this, many of our members work closely with DHS and the U.S. Secret Service to prepare for events of national significance; they also work with the National Security Agency (NSA) and Department of Defense (DOD) on addressing mission-critical electric power needs “on the ground” at the base level and from the national perspective.

Your letter references the voluntary program that the Cyber Security Act of 2012 would have created to “empower the private sector to collaborate with the government and develop dynamic and adaptable voluntary cyber security practices.” We want to be clear that we do not oppose such a regime, provided it does not seek to supplant the existing regulatory structures and public-private coordination already taking place in the electric and nuclear power sectors, even in the absence of new cyber-security legislation.

Since passage of the Energy Policy Act of 2005, the electric sector has been subject to mandatory, enforceable, cyber security standards under the jurisdiction of the Federal Energy Regulatory Commission (FERC), while the Atomic Energy Act and Nuclear Regulatory Commission (NRC) have created a similar regime for nuclear power plants. These standards are constantly evolving and improving as our systems, and the threat environment, change. Given the resources that have been dedicated to the drafting and implementation of these cyber security standards, our members were understandably concerned that any new DHS-centric approach that did not account for the existing FERC and NRC processes could result in conflicting or duplicative standards. Of course there is a role for DHS; we agree they should provide the national security context for FERC and NRC to ensure the industry and regulators are focusing on the right threats. However, as Congress continues to consider legislation, we would urge you to retain the existing sector-specific processes which rely on the technical expertise of industry experts working in conjunction with federal regulators to ensure that cyber security standards are technically and operationally sound, and do not result in unintended consequences.

We also recognize that, while standards enforce good business practices and encourage a baseline level of security, compliance checklists that focus only on performance requirements are not sufficient to address cyber threats. Imminent cyber threats require quick action and flexibility that can come only from close collaboration with the government and emergency response protocols that are planned and practiced before a disaster strikes.

Given the differences of opinion evident in the Senate debate, it may be difficult for Congress to agree on a government-wide framework for cyber security that accounts for all 18 critical infrastructure sectors. We do not believe these differences are insurmountable and look forward

to working with you on a solution. In the meantime, in the absence of consensus, we would encourage Congress to act on legislation improving information-sharing capabilities among government and industry.

We appreciate your efforts, and the efforts of all in Congress who have identified cyber threats as a national security imperative. You undoubtedly will hear company-specific insights from the CEOs of the electric utilities your letter reached, but, given the importance of this issue, we wanted to make you aware that this is a priority shared by all of our members.

Sincerely,



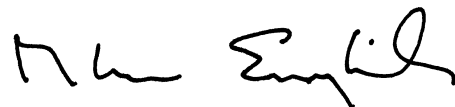
Mark Crisson, CEO
American Public Power Association



Thomas R. Kuhn, President
Edison Electric Institute



John E. Shelk, President & CEO
Electric Power Supply Association



Glenn English, CEO
National Rural Electric Cooperative
Association



Marvin S. Fertel, President & CEO
Nuclear Energy Institute