COMMITTEES

NATURAL RESOURCES
RANKING DEMOCRAT

ENERGY AND COMMERCE

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900

http://markey.house.gov

August 8, 2012

The Honorable Barack Obama
President
1600 Pennsylvania Avenue
Washington, DC 20500

Dear Mr. President,

American's electricity grid is the linchpin of American economic and national security. All of our Nation's critical systems – financial services, health care, telecommunications, transportation, water, defense, law enforcement – depend on the electricity grid. Despite years of thorough investigation and exhaustive hearings in both the House and Senate, it became clear last week that Republicans in Congress will not allow the passage of badly needed legislation to addresses the cyber threats to America's electrical grid. I write today to strongly urge you to take action by executive order to ensure that all necessary measures be taken to secure system reliability when cyber threats and vulnerabilities to the nation's electrical power system are known.

It is unconscionable that Congress has failed to take decisive legislative action to address what should be a non-partisan national security issue. In the last Congress, I, along with Republican Congressman Fred Upton, introduced the GRID Act, which gives FERC the clear authority to issue regulations to combat known cyber-vulnerabilities. That way, we need not be at the mercy of an industry that historically has been inexcusably slow to act. The legislation passed by a vote of 47-0 in Committee and unanimously in the full House of Representatives. The electric utility industry then successfully persuaded Senate Republicans to stall the bill. In this Congress, emboldened by the drumbeat of regulatory repeal that has been the hallmark of the new Republican majority, the electric utility sector has lobbied aggressively against the measure. House Republicans have acceded to industry's desire to simply regulate itself.

From banks to hospitals to police, none of our core public or private institutions can properly function without the grid. Ninety-nine percent of the electric energy used to power our military facilities – including critical strategic command assets – comes from the commercially operated grid. Our dependence on the grid is only deepening as we move towards greater reliance on automation and information technology. A coordinated attack by sophisticated cyber criminals has the potential to knock out all of these systems for weeks or months or even years.

National security experts have warned of an intensifying terrorist threat to America's critical infrastructure. FBI Director Robert Mueller recently warned that cyber-attacks soon will surpass terrorism as the number one threat facing the country. The Department of Homeland

PRINTED ON RECYCLED PAPER

Security has warned that hackers have come close to shutting down portions of our critical infrastructure. Reports of cyber-security incidents at U.S. power plants and other infrastructure skyrocketed nearly 400 percent from 2010 to 2011. And all five Federal Energy Regulatory Commissioners (FERC), the agency with jurisdiction over electrical facilities, have stated in Congressional testimony that they ranked cyber-threats at the very top of their list of threats to electricity reliability.

Regrettably, the utility industry is not doing what it should to combat these threats, and FERC currently lacks the authority to compel it to. As you know, FERC directs the electric utility industry to suggest its own standards to combat cyber-security vulnerabilities. However, there are no hard and fast deadlines with this voluntary approach, and if the industry proposes inadequate measures, all FERC can do is remand the measures for further work. Finalizing reliability standards through this industry-led, consensus-based process typically takes years. It is wholly inadequate for responding to time sensitive threats and vulnerabilities related to infrastructure that is critical to national security.

It took the industry several years to finish writing voluntary recommendations to combat the 2007 "Aurora vulnerability," which could cause key portions of power-plants to self-destruct. Industry has done little to assess the effectiveness of these voluntary measures and has not submitted a single one of them to FERC in the form of a proposed mandatory standard. In 2010, industry issued 12 voluntary recommendations to combat the Stuxnet computer worm, which was used to attack Iran's nuclear centrifuges and which has since been re-designed so it can harm other systems. But industry only agreed to turn five of the 12 recommendations into mandatory standards. And when the FBI warned in 2010 that cyber-intruders could remotely gain access to electric utility assets, an industry vote rejected the majority of their voluntary recommendations be made mandatory.

Leaving America powerless against the threat to the security of our electricity grid is an unacceptable and an unnecessary risk. We should not wait for a crippling terrorist attack on our grid before we act. If Congressional Republicans insist on fully entrusting the safety of our grid to a utility industry that is ill-equipped to adequately and uniformly respond to threats and vulnerabilities that are of paramount importance to national security, then you can and must take action to mitigate these threats and vulnerabilities to the extent possible by executive order.

I thank you for your dedication to this issue, and I look forward to continuing to work with you to ensure the reliability of our nation's electricity grid.

Sincerely,

Edward J. Markey
Member of Congress