United States Senate
WASHINGTON, DC 20510

September 18, 2012

President Barack Obama
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

As we write, the inadequate cybersecurity of our nation's computer systems and networks poses a severe and unaddressed threat to our national and economic security. This risk is particularly acute with respect to the systems found in our critical infrastructure: our nuclear power plants, dams, financial networks, and the electric grid.

We were therefore deeply disappointed that a sufficient number of our colleagues in the Senate chose to block passage of S. 3414, the Cybersecurity Act of 2012. We remain committed to the passage of this important legislation, and are continuing our efforts to resolve differences regarding the appropriate role of government in the protection of critical infrastructure. We write today to stress, however, that the failure of Congress to act should not prevent the executive branch from taking available steps to counter the enormous and growing cyber threat.

Accordingly, we urge you to direct Secretary Napolitano to convene an inter-agency group that will develop, in close collaboration with the private sector, voluntary standards for digital safeguards for our nation's critical infrastructure. We believe that the government and the private sector must work together with great urgency to enhance the cybersecurity of privately held critical infrastructure and had hoped that the widely shared goal of addressing this important national security need would have succeeded in forging a consensus.

Led by the bill's bipartisan sponsors, we have made much progress: supported by a majority of the Senate, the current legislation would establish a voluntary process through which government and industry come together to issue common sense, outcome-oriented standards for achieving an acceptable measure of cybersecurity for critical infrastructure. Unfortunately, a sufficient number of Senators remain opposed to the creation of any government standard — advisory or not — out of a concern that a responsible agency might someday use existing regulatory authority to make such a standard mandatory.

Notwithstanding these objections, the Secretary of the Department of Homeland Security already has authority to issue advisory guidelines under existing statutes (*e.g.*, § 201(d)(6) of the Homeland Security Act of 2002) and we ask that you instruct her to do so.

We recognize that an order directing the promulgation of voluntary standards cannot and should not be the final word in cybersecurity. An executive order, for example, would not be able to provide the types of incentives for participating companies that Congress can establish. A well-crafted set of voluntary standards could, however, be an important step towards improving the cybersecurity of our nation's critical infrastructure.

Another pressing cybersecurity need is the improvement of the quality of information sharing about cybersecurity threats between private sector entities and with government experts. We have worked with a wide array of stakeholders who agree that reform is necessary, but we believe that any reform in this area must be certain to safeguard the privacy rights of U.S. citizens.

Only legislation can replace the existing legal regime — which stifles information sharing — with new laws that are consistent with both the protection of civil liberties and the promotion of cybersecurity. The current legislation makes real and valuable progress in striking a balance with privacy concerns, unlike competing legislative proposals. We are therefore determined to pass comprehensive legislation and remain convinced that S. 3414 is the vehicle for doing so.

Sincerely,

Christopher A. Coons
U.S. Senator

Richard Blumenthal
U.S. Senator