

DANIEL K. INOUE, HAWAII
JOHN F. KERRY, MASSACHUSETTS
BARBARA BOXER, CALIFORNIA
BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
FRANK R. LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
TOM UDALL, NEW MEXICO
MARK WARNER, VIRGINIA
MARK BEGICH, ALASKA

KAY BAILEY HUTCHISON, TEXAS
OLYMPIA J. SNOWE, MAINE
JIM DEMINT, SOUTH CAROLINA
JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
JOHNNY ISAKSON, GEORGIA
ROY BLUNT, MISSOURI
JOHN BOOZMAN, ARKANSAS
PATRICK J. TOOMEY, PENNSYLVANIA
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
DEAN HELLER, NEVADA

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: <http://commerce.senate.gov>

ELLEN DONESKI, STAFF DIRECTOR
BRIAN M. HENDRICKS, REPUBLICAN STAFF DIRECTOR AND GENERAL COUNSEL

August 13, 2012

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

Dear Mr. President:

I am profoundly disappointed that the United States Senate failed to enact comprehensive cybersecurity legislation last month. I cannot recall a circumstance throughout my years in the Senate in which a filibuster has obstructed genuine efforts to address a threat to our national security that is so urgent and widely recognized, where the military and intelligence advice was so explicit and urgent, and where the bipartisan national security consensus was so deep and broad.

This filibuster constituted an outright rejection of the advice of our top military officials – including the Chairman of the Joint Chiefs of Staff, General Martin Dempsey, and the head of the National Security Agency and Cyber Command, General Keith Alexander, both of whom had personally urged immediate action on cybersecurity legislation. Both our military brass and a wide variety of national security experts across the political spectrum have personally advocated for cybersecurity legislation because they believe the cyber threat to our nation is real and immediate. I share their concerns.

The cosponsors of the Cybersecurity Act will continue to advocate for legislation in the Senate and will encourage other Senators to reconsider the position they took last month. However, because it is very unclear whether the Senate will come to agreement on cybersecurity legislation in the near future, I urge you to explore and employ every lever of executive power that you possess to protect this country from the cyber threat. We must act to address our cyber vulnerabilities as soon as possible and many components of the Cybersecurity Act are amenable to implementation via Executive Order, normal regulatory processes, or other executive action under the authorities of the Homeland Security Act. You have my strong support to take steps necessary to protect our country.

In particular, I believe you can issue an Executive Order to establish a program to protect critical cyber infrastructure along the lines of the program that we proposed in Title I of the Cybersecurity Act. This program would have created a collaborative partnership between the private sector and the federal government to conduct cyber risk assessments of our nation's most critical infrastructure and create voluntary best practices for companies to implement. The program also included incentives for adopting the practices, including protection against liability

for punitive damages. While a program created through executive action cannot include such incentives, I believe it is critical that we move forward.

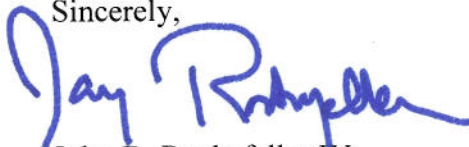
Such a program should be premised on private sector leadership and accountability, with government assistance and guidance as necessary. It should place a focused priority on protecting critical systems whose incapacitation or disruption could cause catastrophic damage to the United States. To address our country's most pressing cyber vulnerabilities, this program should:

- Begin with a comprehensive and collaborative government-private sector risk assessment to inventory the threats and vulnerabilities that pose particular risks to particular categories of critical infrastructure;
- Draw on government and private sector expertise to develop dynamic and adaptable cybersecurity practices that are best suited for each critical infrastructure sector; and
- Implement these practices through private sector collaboration with, and assistance from, an interagency effort that includes the Departments of Defense, Commerce, and Justice, as well as other sector-specific agencies and regulators, and is led by the Department of Homeland Security.

I believe companies that own critical infrastructure will choose to participate in this program because it will be their best option to protect themselves against the cyber threat facing our nation. This cyber threat is unprecedented and we need an innovative and cooperative approach between the private sector and the federal government to protect the country from it.

Please let me know if I can provide any assistance as you consider this decision.

Sincerely,



John D. Rockefeller IV
Chairman