JOHN D. ROCKEFELLER IV, WEST VIRGINIA, CHAIRMAN

DANIEL K. INOUYE, 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

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

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

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

September 19, 2012

Mrs. Virginia M. Rometty
President and Chief Executive Officer
International Business Machines
1 New Orchard Rd.
Armonk, NY 10504

Dear Mrs. Rometty:

I was profoundly disappointed that the United States Senate's effort to pass comprehensive cybersecurity legislation was blocked by a partisan filibuster last month. The cyber threats we face are real and immediate, and Congress's failure to pass legislation this year leaves the country increasingly vulnerable to a catastrophic cyber attack. Because of the urgency of the need to address this threat, in August following the Senate's failure to act, I urged President Obama to use his authority to implement cybersecurity protections for our country through an Executive Order.

While I believe an Executive Order is a step in the right direction, I believe the President will be able to accomplish through an Executive Order only a portion of what the Cybersecurity Act of 2012 set out to do. Legislation will still be needed and I would like to hear directly from our nation's business community to understand their views on cybersecurity. I am writing to our country's five hundred largest companies because the filibuster of the legislation in the Senate was largely due to opposition from a handful of business lobbying groups and trade associations, most notably the United States Chamber of Commerce. I have spoken with several business executives about these issues, and I believe that most recognize the gravity of this threat and that their companies would benefit from deeper collaboration with the government. I would like to hear more – directly from the chief executives of leading American companies about their views on cybersecurity, without the filter of beltway lobbyists.

Many companies have worked closely with us for years to develop and refine our bill. Even those companies that have been more critical have offered us constructive input that has improved the legislation. I would be surprised to learn that many other American companies, most of which recognize that what is good for their bottom lines is also good for the country's national and economic security, are as intransigently opposed to our cybersecurity legislative efforts as the Chamber of Commerce has indicated they are.

Our country's top military officials, including the Chairman of the Joint Chiefs of Staff and the head of the National Security Agency, have personally asked the Senate to pass cybersecurity legislation because of the severity of the cyber threat we face. I am attaching recent correspondence from both of them for your reference. General Keith Alexander, who as

the leader of both the NSA and the Department of Defense's Cyber Command, has the best vantage point in the country to see the cybersecurity threat, recently stated that "we simply cannot afford further delay" and that "the time to act is now" on cybersecurity legislation. General Martin Dempsey, our nation's top military officer, added his voice to General Alexander's, urging "immediate passage of comprehensive cybersecurity legislation," and stating that "we must act now."

Scores of national security experts, both Republican and Democrat, agree and have repeatedly called for the Senate to pass cybersecurity legislation. Yet for reasons I do not understand, the Chamber of Commerce and other business lobbying groups opposed our plan to create a voluntary program that would empower the private sector to collaborate with the federal government to develop dynamic and adaptable voluntary cybersecurity practices for companies to implement as they see fit. This private sector-led approach strikes me as one that companies would want to have codified in statute, rather than risking reactive and overly prescriptive legislation following a cyber disaster.

I have been pushing cybersecurity legislation for years because I believe that our country would be more secure if American companies implemented cybersecurity practices that were developed to address their particular cyber vulnerabilities. The cyber threat we face is unprecedented and we need an innovative and cooperative approach between the private sector and the federal government to protect the country from it. We need expertise and leadership from both the federal government and the private sector to keep our country, our businesses and our citizens safe and secure.

To help me understand your company's views on cybersecurity, I ask that you provide responses to the following questions by Friday, October 19, 2012.

1. Has your company adopted a set of best practices to address its own cybersecurity needs?

2. If so, how were these cybersecurity practices developed?

3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.

4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?

5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?

6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity

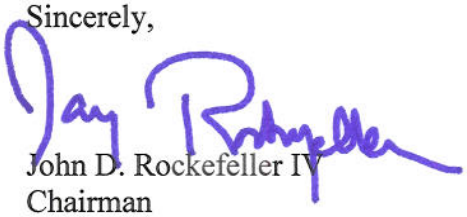
practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?

7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?

8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

If you have any questions, please contact Ellen Doneski or Erik Jones with my staff at (202) 224-1300. Your response can be filed with the Committee via the following e-mail address: cybersecurity@commerce.senate.gov.

Sincerely,



John D. Rockefeller IV
Chairman