

BARBARA BOXER, CALIFORNIA
BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
FRANK R. LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
MARK WARNER, VIRGINIA
MARK BEGICH, ALASKA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII

JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
ROY BLUNT, MISSOURI
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
DEAN HELLER, NEVADA
DAN COATS, INDIANA
TIM SCOTT, SOUTH CAROLINA
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
RON JOHNSON, WISCONSIN

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

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

ELLEN DONESKI, STAFF DIRECTOR
DAVID SCHWIETERT, REPUBLICAN STAFF DIRECTOR

June 3, 2013

The Honorable Cameron F. Kerry
Acting Secretary
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

Dear Acting Secretary Kerry:

As a strong supporter of the Department of Commerce's role in strengthening our country's cybersecurity, I am responding to the Department's March 28, 2013, request for comments about promoting the adoption of the framework to reduce cyber risks to critical infrastructure (the "Framework") that the National Institute for Standards and Technology (NIST) is currently developing.

I am very pleased that Executive Order 13636 gives NIST the lead role in developing the Framework. Because of its technical expertise and its well-earned reputation as an "honest broker" in the standards development process, NIST is the right institution to lead the effort to reduce cyber risks. Cybersecurity legislation that the Senate Commerce Committee considered and reported in the 111th Congress (S. 773) took a similar approach to developing cybersecurity standards. This bipartisan legislation called on NIST to engage the private sector in a process to develop cyber risk management techniques and best practices.

The Obama Administration's preference for a NIST-coordinated, private sector-driven process for developing cybersecurity standards sends a clear message that public-private collaboration is the most effective way to strengthen our cyber defenses. I strongly support this approach and continue to believe that Congress should formally endorse it in legislation.

Unlike a federal agency engaged in a regulatory rulemaking process, NIST's purpose in bringing together knowledgeable players from government and industry is to support their efforts to build consensus around common technical standards. By definition, the NIST standards-making process is a collaborative effort between industry and government. Industries adopt NIST standards not because they are required to, but because the standards that emerge from the NIST process consistently have high technical quality and utility. There are many well-documented cases where NIST standards have improved the quality of goods and services

produced by U.S. companies, while lowering transaction costs and promoting innovation.¹ In addition to the important role it plays in developing standards in the United States, NIST also actively works to harmonize U.S.-based standards with international standards.

Because of this, I believe the single strongest incentive for operators of critical infrastructure and other interested entities to adopt the Framework will be the creation of the Framework itself. Developed through a transparent process in which industry stakeholders share their cybersecurity challenges and solutions, the Framework will represent our country's very best current thinking on how to address and measure cybersecurity risks. U.S. companies will adopt the Framework because it will be a powerful new cyber risk management tool; they will implement the Framework's standards to demonstrate to their investors, business partners and insurers that they are implementing the best cybersecurity practices available in their industry sector.

The more information the NIST process can provide market players about cybersecurity solutions, the stronger the incentives will be to adopt the Framework. For instance, companies would benefit from further precision in metrics and measurements of the financial costs and benefits of various cybersecurity postures. Improved methodologies for more precise valuation and loss estimates regarding businesses' cybersecurity considerations – including secure intellectual property, confidential contract negotiations and bidding documents, and resilient business and industrial control systems – would aid companies in prioritizing their cyber investments and insuring against cyber losses.

The Framework will give companies, investors, and insurers important new insights for evaluating cybersecurity risks and efficiently allocating their resources. As I have written to Mary Jo White, Chairman of the Securities and Exchange Commission, I believe that investors should be properly informed about material cyber risks and events that an investment target company faces, and, most importantly, the steps that company is taking to address those particular risks.² The more precise the metrics regarding the costs and benefits of various cyber investments, the more informed and efficient the market will be in allocating capital to the benefit of cybersecurity.

I also agree with the Department of Commerce Internet Policy Task Force in its description of cybersecurity insurance as a potentially “effective, market-driven way of increasing cybersecurity,” and I believe that the nascent but fast-developing market for private insurance will be key to managing cyber risks in the future. As of now, however, in the absence of a framework like the one that NIST is presently developing, and without more precise valuation/loss metrics, the cyber insurance market suffers from a lack of clear standards of care and actuarial calculations. The standards and guidelines developed through the current

¹ See e.g., Erik Puskar, *Selected Impacts of Documentary Standards Supported by NIST, 2008 Edition*, NISTIR 7548 (Jan. 2009); David Leach and John T. Scott, *The Economic Impacts of Documentary Standards: A Case Study of the Flat Panel Display Measurement Standard (FPDM)*, CGR G2012-0299 (Dec. 2011).

² Letter from John D. Rockefeller IV, to Mary Jo White, Chairman, Securities and Exchange Commission (April 9, 2013) (online at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51).

The Honorable Cameron F. Kerry
June 3, 2012

Framework process will help insurers quantify cyber risks, and reward companies that adopt best practices to mitigate these risks.

Finally, I do not believe that giving U.S. companies prospective liability protections for adopting the Framework will encourage U.S. companies to improve their cybersecurity. In fact, such an approach would likely have the opposite effect. Again, the outcome of the NIST-convened Framework process will be driven and determined by industry; in turn, companies will adopt the Framework if the product of this private-sector led effort benefits their security and business operations. Giving companies unprecedented prospective liability protections based on cybersecurity standards that they themselves have developed would increase the likelihood that the American taxpayers will one day find themselves on the hook for corporate bailouts of unknown size or scope following a cyber disaster.

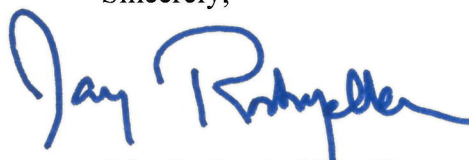
Blanket liability protections for adopting the Framework would have at least five negative outcomes: Such protections would create perverse incentives to craft low-bar standards; create the moral hazard of an incentive for a company to perform nothing more than the minimum standard; undermine companies' ability to negotiate and enforce cybersecurity terms through contractual agreements; frustrate attempts to determine legal accountability following an actual disaster; and, perhaps most importantly, undermine and otherwise distort the private market for cyber insurance.

In short, such liability protections would turn existing market incentives for implementing cybersecurity best practices on their head. Prospectively relieving companies from responsibility for the massive costs that a failure to manage cybersecurity risks might someday impose on American society discourages, rather than promotes, the Executive Order's goal of improved cybersecurity.

I am also concerned about the impact granting legal protections based on the adoption of the Framework will have on NIST's reputation as a non-regulatory, technical and scientific agency. The value NIST contributes to any standard-developing process depends on its role as an "honest broker" in the process, as a participant that has no interest other than developing the best possible technical standards. Conferring significant financial benefits on companies that adopt NIST's Framework puts the agency in a quasi-regulatory role, and risks undermining the agency's core statutory mission of enhancing American competitiveness.

Thank you for your consideration of my perspectives on these important matters, and I look forward to working with you to complete and promote the Framework.

Sincerely,



John D. Rockefeller IV
Chairman