United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 26, 2012

Dear Colleague:

Last week we introduced a new version of the Cybersecurity Act of 2012 (S.3414), which makes substantial revisions to the cybersecurity bill (S. 2105) we introduced in February. Although we still prefer the stronger protections in our original bill, we made these changes in a sincere attempt to accommodate concerns raised by our colleagues. We are writing today to explain the changes, refute the misinformation that has been circulating about the bill, and to seek your support.

Our revised bill sets up a public-private partnership, establishing a National Cybersecurity Council, an interagency body with members from the Departments of Defense, Justice, Commerce, the intelligence community, appropriate sector-specific Federal agencies, and appropriate Federal agencies with responsibilities for regulating the security of covered critical infrastructure. This Council would be chaired by the Department of Homeland Security and work in partnership with the private sector. The Council would be charged with conducting sector-by-sector risk assessments to identify cyber risks and, in doing so, would identify particular categories of critical infrastructure as critical cyber infrastructure. The Council could only identify categories of infrastructure as critical cyber infrastructure if a cyber attack to that infrastructure could reasonably be expected to result in a mass casualty event, mass evacuations, catastrophic economic damage to the United States, or severe degradation of national security. Owners of this absolutely critical infrastructure would be required to report significant cybersecurity incidents to help protect our national security from any consequences of such attacks and to help protect other critical infrastructure from similar attacks.

The bill provides that the private sector (working through existing sector coordinating councils) would develop and propose to the Council voluntary, outcome-based cybersecurity best practices, which the Council would review and then adopt or modify or supplement as necessary to ensure the identified risks are mitigated by the cybersecurity practices. To provide incentives for private sector owners to implement the voluntary cybersecurity practices, the Council would develop a voluntary cybersecurity program. Contrary to critics' claims, neither members of the sector coordinating councils nor anyone else will be required to adopt these voluntary practices. Owners wishing to join the program would have the choice, either through self-certification or through a third party assessment, whichever makes the most sense for their business, to demonstrate they have implemented measures of their choosing that satisfy the cybersecurity practices. Recognizing that industry owners and operators are in the best position to know which methods and processes are right for their sector, participating owners would have complete flexibility over the manner in which these cybersecurity practices are met. In fact, these practices cannot prescribe specific products, or their design or development. Owners that join the program would receive certain benefits such as liability protection from any punitive damages associated

with a cyber incident, eligibility for an expedited security clearance process for appropriate personnel employed by the certified owner, and prioritized technical assistance on cyber issues.

Some have charged that our bill authorizes "open-ended, undefined regulatory schemes." Not so. The Council's authority is carefully focused on conducting a risk assessment and adopting voluntary cybersecurity standards after review of proposals from the sector coordinating councils. This bill creates no new regulators, and provides no new authority for an agency to establish standards that is not otherwise already authorized by law.

Some have argued that cybersecurity legislation should not include any measures to help protect our most critical infrastructure from cyber attacks and should rely completely on information sharing – the sharing of information regarding specific cyber threats. While our bill contains strong information sharing provisions, information sharing alone is not enough to address this threat. Many critical systems do not have the appropriate security practices in place to use information shared with them or to gather their own information to share with others. If critical infrastructure systems don't have the capabilities or wherewithal to act on timely information or fail to attempt to gather information about threats to share with others, then sharing real-time intelligence with them won't do much good. As NSA Director General Keith Alexander recently said, for information sharing to add value, the entity sharing the information must have some basic capacities that are currently lacking in many critical systems. In addition, both senior civilian and military leadership have said our revised bill satisfies the operational needs of every federal agency with a cybersecurity mission.

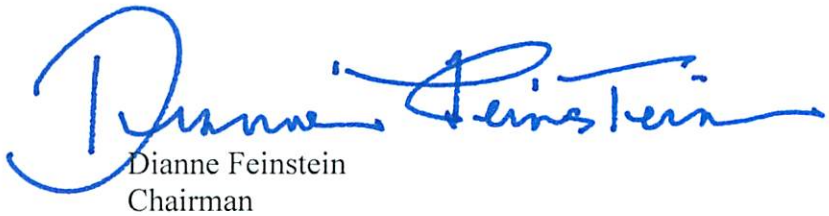
Our critical infrastructure is increasingly vulnerable to cyber threats, and the destruction or exploitation of critical infrastructure through a cyber attack, whether a nuclear power plant, a region's water supply, or a major financial market, could cripple our economy, undermine the safety of our transportation and utilities, and throw our country into chaos. Recent attacks on our natural gas pipelines clearly illustrate the threat. The number of attacks against critical infrastructure reported to the Department of Homeland Security increased by 383 percent in the last year alone. Numerous national security experts from both parties have concluded cybersecurity legislation must provide protections for critical infrastructure and have actually advocated for measures much stronger than included in this bill. This week, 18 members of the Homeland Security Group of the Aspen Institute, leaders in the fields of homeland security, national security, intelligence, and law, joined together to strongly praise and urge action on our bill in a letter we have enclosed. We can no longer afford to ignore the threat to our critical infrastructure posed by cyber vulnerabilities and must act now. Please join us in supporting our revised Cybersecurity Act of 2012 in the interest of protecting our national and economic security.

Sincerely,

Joseph I. Lieberman
Chairman
Senate Committee on Homeland Security
and Governmental Affairs

Susan M. Collins
Ranking Member
Senate Committee on Homeland Security
and Governmental Affair

John D. Rockefeller IV
Chairman
Senate Committee on Commerce,
Science, and Transportation



Dianne Feinstein
Chairman
Senate Select Committee on Intelligence

Tom Carper
Chairman
Subcommittee on Federal Financial
Management, Government Information,
Federal Services and International Security
Senate Committee on Homeland Security
and Governmental Affairs

THE ASPEN INSTITUTE
HOMELAND SECURITY GROUP

STATEMENT OF THE ASPEN HOMELAND SECURITY GROUP (July 24, 2012)

The Aspen Homeland Security Group strongly urges the U.S. Senate to vote this week to take up S3414, the cyber-security bill, for debate on the floor. We urge the Senate to adopt a program of voluntary cyber-security standards and strong positive incentives for critical infrastructure operators to implement those standards. The country is already being hurt by foreign cyber-intrusions, and the possibility of a devastating cyber-attack is real. Congress must act now.

Charles E. Allen

Stewart A. Baker

Richard Ben-Veniste

Peter Bergen

Michael Chertoff

P.J. Crowley

Clark K. Ervin

Jane Harman

Michael V. Hayden

Michael Leiter

James M. Loy

Paul McHale

John McLaughlin

Phillip Mudd

Eric T. Olson

Guy Swan III

Juan Zarate

Philip Zelikow