

JOSEPH I. LIEBERMAN, CONNECTICUT, CHAIRMAN

CARL LEVIN, MICHIGAN  
DANIEL K. AKAKA, HAWAII  
THOMAS R. CARPER, DELAWARE  
MARK L. PRYOR, ARKANSAS  
MARY L. LANDRIEU, LOUISIANA  
BARACK OBAMA, ILLINOIS  
CLAIRE McCASKILL, MISSOURI  
JON TESTER, MONTANA

SUSAN M. COLLINS, MAINE  
TED STEVENS, ALASKA  
GEORGE V. VOINOVICH, OHIO  
NORM COLEMAN, MINNESOTA  
TOM COBURN, OKLAHOMA  
PETE V. DOMENICI, NEW MEXICO  
JOHN WARNER, VIRGINIA  
JOHN E. SUNUNU, NEW HAMPSHIRE

MICHAEL L. ALEXANDER, STAFF DIRECTOR  
BRANDON L. MILHORN, MINORITY STAFF DIRECTOR

# United States Senate

COMMITTEE ON  
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

June 25, 2010

Susan Herman  
President, American Civil Liberties Union  
Attention: Michelle Richardson, Legislative Consultant  
915 15<sup>th</sup> Street, NW  
Washington, DC 20005

Dear Ms. Herman:

Thank you for the opportunity to discuss issues relating to the privacy and civil liberties aspects of the Protecting Cyberspace as a National Asset Act, S. 3480.

This Committee has long been engaged in matters relating to privacy and civil liberties, and we believe that this legislation continues our efforts to balance the needs of transparency and openness in government while protecting the privacy and civil liberties of the American people. We are sure you would agree that improved cybersecurity will, among other things, significantly improve privacy protections and safeguard the personally identifiable information (PII) of all Americans. Indeed, the PII of over 30 million Americans has already been lost or stolen from government databases due to lax information security.

Our bill contains significant measures to safeguard privacy and civil liberties, and yesterday we were pleased to receive a letter from the Center for Democracy and Technology, a signatory to your letter, recognizing "the open, collaborative process" we fostered to consider suggestions such as yours, and approving of the "significant changes" we made as a result of that process.

Because your letter was drafted without the benefit of the substitute amendment, we would like to highlight several provisions, as well as some that were in the bill as introduced on June 10, 2010, that we believe address many of your concerns.

**Scope.** Instead of expansive new authorities relating to cybersecurity, S. 3480 seeks to add precision and focus to complement existing law. Our bill specifies that only those systems or assets whose disruption would cause a national or regional catastrophe would be subject to the bill's mandatory security requirements. Thus, the bill sets up a process that clearly defines – and limits – the systems and assets that the Department of Homeland Security (DHS) can identify as covered critical infrastructure.

To qualify as a national or regional catastrophe, the disruption of the system or asset would have to cause:

- mass casualties with an extraordinary number of fatalities;
- severe economic consequences;
- mass evacuations of prolonged duration; or
- severe degradation of national security capabilities, including intelligence and defense functions.

Additionally, owners/operators who believe their systems and assets were erroneously added to the DHS list of covered critical infrastructure will have an opportunity to appeal their inclusion through administrative procedures. Both of these additions help ensure that a targeted slice of the critical infrastructure is covered. Thus, we do not believe that the scope of covered critical infrastructure is overly broad.

**Preserving Free Speech in Cybersecurity Emergencies.** The bill specifically includes strong provisions to protect free speech in the time of an emergency. In Section 254(a)(3) of the substitute amendment, we would expressly prohibit the Secretary of DHS from identifying systems or assets as covered critical infrastructure “based solely on activities protected by the First Amendment of the United States Constitution.”

Additionally, Section 249(a)(6)(A) of the bill expressly prohibits the Director of the National Center for Cyber Security and Communications (NCCC), DHS or any other Federal entity to “restrict or prohibit communications carried by, or over, covered critical infrastructure and not specifically directed to or from the covered critical infrastructure unless the Director determines that no other emergency measure or action will preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption of the covered critical infrastructure or the national information infrastructure.”

Section 249 of the original bill already included language requiring that any imposed emergency measures be the “least disruptive means feasible” in order to secure the covered network. The substitute amendment expands the “least disruptive means” analysis to require an examination of the broader impact an emergency measure would have on the overall national information infrastructure. This section also expressly requires that the privacy and civil liberties of the American people are protected.

The Lieberman-Collins-Carper substitute amendment makes another significant change limiting the President’s power in a cybersecurity emergency: the 30-day period for imposing emergency measures cannot be renewed indefinitely. Instead, Congress would have to approve an extension of the emergency authorities beyond 120 days. Taken together, we believe these provisions reflect a sensible, balanced approach and more than meet the First Amendment strict scrutiny test.

**Information Sharing and Privacy.** One key goal of the bill is to increase the ability of information to be shared related to cyber security to better respond to threats. While we have developed new requirements to report incidents, the language is carefully tailored so that the

reporting does not lead to the disclosure of PII. Section 246(b)(2)(C) requires that incident reports include appropriate mechanisms to protect personally identifiable information. The bill would require the Director of the NCCC to develop specific guidelines to protect the privacy and civil liberties of people living in the United States, which would be done in conjunction with the privacy officer of the NCCC. In addition, the Committee intends to include report language to specify that these activities should be conducted consistent with Fair Information Practices developed by DHS.

**Transparency.** Our committee agrees that transparency relating to cybersecurity is vitally important. But we also believe the increased cyber security depends in part on more information being shared about the nature of the threats we face and the government's efforts to defend against those threats. That is one of the reasons why we believe DHS should be the lead civilian agency for cybersecurity and that the Director of the White House Office of Cyberspace policy must be accountable, and therefore confirmed by the Senate. DHS also has worked to provide security clearances to civil liberties and privacy advocates from around the country who will continue to ensure that civil liberties and privacy protections are included every step of the way.

A significant report required by our bill will further increase transparency by mandating that the Director of the Cyberspace Policy Office at the White House describe "the activities, ongoing projects, and plans of the Federal Government designed to meet the goals and objectives of the National Strategy [to increase the security and resiliency of cyberspace]." Section 107(c) of our bill requires that the reports be made available to the public in an unclassified form. Additionally we require a report on US-CERT's activities to be provided in an unclassified form to allow it to be shared widely. To emphasize transparency further and emphasize the need for public involvement in cybersecurity, Section 246(d) allows for creation of a mechanism by which the public can comment and suggest improvements to the policy and operations of the NCCC.

Some additional privacy and civil liberty provisions of the bill include:

- A requirement that the National Strategy relating to cyberspace security and resiliency include privacy and civil liberties;
- Numerous requirements for consultation with the Privacy and Civil Liberties Oversight Board and the Information Security and Privacy Advisory Board within the White House, DHS, and other federal agencies;
- The creation of a full-time privacy officer to consult on cyber security matters within DHS;
- An OMB review of existing policies relating to current privacy requirements for the federal government.

Thank you for sharing your concerns on this important issue and for giving us the opportunity to respond. We are committed to an open dialogue on this bill with all stakeholders involved in this important legislation. We look forward to working with all of you going forward.

Sincerely,



Joseph I. Lieberman  
Chairman



Susan M. Collins  
Ranking Member



Thomas R. Carper  
Chairman, Subcommittee on Federal Financial Management,  
Government Information, Federal Services, and  
International Security

CC:

American Library Association  
American Association of Law Libraries  
Association of Research Libraries  
Bill of Rights Defense Committee  
Center for Democracy & Technology  
Citizens Committee for the Right to Keep and Bear Arms  
Competitive Enterprise Institute  
Constitution Project  
Cyber Privacy Project  
Defending Dissent Foundation  
DownsizeDC.org  
Electronic Frontier Foundation  
Government Accountability Project  
Liberty Coalition  
Liberty Guard  
Muslim Public Affairs Council  
Muslimah Writers Alliance  
National Lawyers Guild – National Office  
OpenTheGovernment.org  
OMB Watch  
Political Research Associates  
Rutherford Institute  
U.S. Bill of Rights Foundation