KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

June 24, 2010

The Honorable Joseph Lieberman, Chairman
The Honorable Susan Collins, Ranking Member
The Honorable Tom Carper
Senate Committee on Homeland Security and Government Affairs
340 Dirksen Senate Office Bldg.
Washington, D.C. 20510

Re: S. 3480, the Protecting Cyberspace as a National Asset Act

Dear Chairman Lieberman, Ranking Member Collins and Senator Carper:

We are writing to express the views of the Center for Democracy & Technology[1] on the substitute amendment to the Protecting Cyberspace as a National Asset Act of 2010. The amendment, which will be offered as a substitute for the underlying bill at a Committee on Homeland Security and Government Affairs mark-up scheduled for today, improves and strengthens the legislation in several respects.

Your legislation is thoughtful, sophisticated and comprehensive. It takes a risk-based approach designed to focus cybersecurity measures where they will do the most good. It does not put the National Security Agency or the Department of Defense in charge of cybersecurity operations respecting civilian government systems or privately held critical infrastructure, which would threaten transparency essential to the success of many cybersecurity initiatives. It also creates a statutory privacy officer at the NCCC and requires consultation with that official, and with the DHS Information Security and Advisory Privacy Board.

It reflects the open, collaborative process your staff maintained since shortly before the bill was introduced on June 10. You were willing to consider proposals that CDT and other stakeholders suggested, and you made significant changes. Focusing on Title II of the bill, we discuss those changes, and some lingering concerns, below.

The bill's most extensive obligations fall on owners and operators of "covered critical infrastructure," making CCI a key term in the legislation. They have to share incident information, certify compliance with security measures that a newly-created DHS National Center for Cybersecurity and Communications ("NCCC") would recognize, submit to evaluations, and implement emergency

1 CDT is a non-profit, non-partisan organization dedicated to keeping the Internet open, innovative and free.

measures that the NCCC requires. The requirements imposed could be quite prescriptive and have a substantial impact on innovation and business practices. Compliance is mandatory and could be expensive; unspecified civil penalties apply for failure to comply.

The substitute clarifies the definition of Covered Critical Infrastructure. As amended, CCI would be a system or asset the destruction or disruption of which would cause national or regional catastrophic effects. A system or asset would not be CCI unless it appeared on a DHS prioritized infrastructure list because, among other things, disruption or destruction would cause an extraordinary number of fatalities, severe economic consequences, mass evacuations with a prolonged absence, or severe degradation of national security capabilities. While we would have preferred tighter language, the intent to limit the scope of CCI is clear, and much more so than in the bill as introduced. The bill as amended would also permit an owner or operator of CCI to appeal such designation administratively – a welcome addition given the economic stakes of such designation – but adverse decisions are not appealable to federal courts. We urge you to permit such appeals.

The bill as amended would authorize the President to declare a national cyber emergency that would trigger authority of the NCCC to "develop and coordinate emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of potential disruption, of covered critical infrastructure." We are concerned about the scope of this authority because the activity that can be compelled is not specified. We urge you to specify the actions that are intended to be authorized.

Though it lacks this specificity, the emergency section already includes some important limitations. First, it specifically indicates that the emergency authorities it bestows do not trump the privacy protections in the electronic surveillance statutes. Second, unlike the bill as introduced, it limits to 120 days (in 30-day increments) the duration of the emergencies the President can declare absent Congressional authorization. Third, unlike the bill as introduced, it prohibits the government from "… restricting or prohibiting communications carried by, or over, covered critical infrastructure and not specifically directed to or from the covered critical infrastructure unless the [NCCC] determines that no other emergency measure or action" will preserve the operation or mitigate the disruption of the CCI or the national information infrastructure. While this implies some authority to shut down or limit Internet traffic that raises some concern, it targets and cabins this authority to limit disruption, and is a welcome addition to the bill.

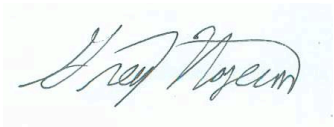
The bill would also empower the NCCC to require that private sector owners and operators of covered critical infrastructure report cybersecurity incidents. Because incident reporting can impact privacy interests, mandatory reporting requirements should be carefully considered. The bill already includes a critically important privacy protection: the incident reporting provisions do not authorize electronic surveillance beyond that authorized in existing law. We urge that you supplement this protection by narrowing the overbroad definitions of "incident" and "information infrastructure," and by requiring that information sharing activities comport with Principles of Fair Information Practices as recognized by DHS.

Finally, the bill would authorize the US Computer Emergency Readiness Team at DHS to provide continuous automated monitoring of Internet traffic to and from

federal agencies at *external* Internet access points. Because this monitoring would be done at the provider level instead of on the agency's own facilities, it raises concern that communications other than those to and from government agencies will be monitored for malicious code. We urge that you clarify that this monitoring cannot extend to private-to-private communications. The bill as introduced wisely included an audit of this monitoring activity; the substitute improves upon the audit requirement by making it clear that the audit should focus on whether private-to-private communications are being monitored, and by ensuring that the results will be reported publicly.

As the bill advances through Congress, we look forward to working with you, and with other Congressional committees, to further clarify, refine and improve a few provisions of the Protecting Cyberspace as a National Asset Act. We view the clarifications and refinements we will seek as necessary additions to legislation already much improved as a result of the collaboration you and your staff have welcomed.

Sincerely,



Gregory T. Nojeim, Director, Project on Freedom, Security & Technology

cc:

Members of Senate Committee on Homeland Security and Government Affairs

The Hon. Jay Rockefeller, Chairman, Commerce Committee

The Hon. Olympia Snowe, Commerce Committee

Chairman Patrick Leahy and Ranking Member Jeff Sessions, Committee on the Judiciary