May 14, 2012

Dear Senator,

We, the undersigned organizations, write to express our deep concerns with S. 2151, the SECURE IT Act of 2012. In particular, we are concerned that the information-sharing provisions in Title I allow companies, "notwithstanding any law," to share sensitive Internet and other information with the government without sufficient privacy safeguards, oversight or accountability.

We understand that cybersecurity legislation will be on the Senate floor soon and that some may consider S. 2151 as a viable alternative to the Cybersecurity Act, S. 2105. In our view, SECURE IT is no such thing in its current form, because the bill poses the following threats to privacy and civil liberties:

- SECURE IT undermines privacy and cybersecurity by authorizing companies to "use cybersecurity systems" to monitor their clients' and customers' Internet usage for broadly-defined "cyber threat information," by authorizing ill-defined "countermeasures" against completely undefined "cybersecurity threats," and by immunizing companies against liability for monitoring activities and countermeasures that violate their own contractual obligations.

- SECURE IT creates an exemption from all existing privacy and tort laws to allow companies to share communications and records with the government, including those of undefined "malicious cyber actors" even if those personal records are not necessary to describe a cybersecurity threat.

- SECURE IT permits companies to share the virtually limitless category of private information that "fosters situational awareness" of the U.S. security posture unless a law specifically protects such information.

- SECURE IT, unlike the Cybersecurity Act (S. 2105), lacks a requirement that companies make reasonable efforts to remove personally identifiable information unrelated to a cybersecurity threat before they share information for cybersecurity purposes.

- SECURE IT does not include any meaningful requirements to ensure that private information is anonymized where possible and to minimize the impact of information sharing on privacy and civil liberties; the bill only requires that the government handle information "in a reasonable manner, including consideration" of privacy rights.

- SECURE IT explicitly designates the NSA and other defense agencies as cybersecurity centers, thereby facilitating the sharing of private information directly with the military.

- SECURE IT, unlike the Cybersecurity Act, requires federal cybersecurity centers that receive cyber threat information to share it immediately with NSA and other military cybersecurity centers, thereby nullifying a company's choice to share user or customer information with a civilian, rather than a military agency.

- SECURE IT, unlike the Cybersecurity Act, allows information shared with the government for cybersecurity purposes to be used for national security reasons unrelated to cybersecurity, and the bill also allows information to be broadly shared and used to investigate and prosecute the many crimes for which a wiretap can be sought (albeit not for all crimes, as in the Cybersecurity Act, unless authorized by the sharing company)—thus circumventing longstanding Fourth Amendment protections that require warrants or other processes designed to protect privacy.

- SECURE IT lacks key meaningful, independent oversight provisions such as mandatory Inspector General reviews; the only oversight required is reports by the agencies involved in the activities the bill authorizes, some of which must be coordinated with the Privacy and Civil Liberties Oversight Board, an entity which will only come into existence if the Senate confirms the five nominees to the Board.

- SECURE IT grants blanket legal immunity to entities that share information, effectively overriding even the contracts companies make with their customers, preventing them from competing on privacy grounds through enforceable promises to their users to protect privacy and by failing to give customers effective legal recourse for violations of what few privacy protections the bill offers.

- SECURE IT, unlike the Cybersecurity Act, does not bar the government from conditioning its disclosure of cyber threat information to a private entity on the entity's provision of cybersecurity threat information to the government, nor does it bar the government from using federal grants or contracts to coerce such sharing; thus, under SECURE IT, information sharing by companies may not be truly voluntary.

- SECURE IT even *requires* companies with contracts to provide communications services to the government to furnish the government with cyber threat information directly related to those contracts even if they collect that information on private networks in the service of other clients, thus undermining private sector autonomy and creating a substantial incentive to overshare private information.

- SECURE IT, like the Cybersecurity Act, lacks meaningful mechanisms – such as recourse for aggrieved individuals – to ensure that governmental agencies use and disclose information shared with them under the bill only as authorized by the bill, creating a risk of routine violation of the limited rules and restrictions contained in the bill.

Therefore, because the bill raises such fundamental civil liberties issues, we urge you to oppose SECURE IT, S. 2151, in its current form. It does not address the concerns many of us have raised with the Cybersecurity Act, and in some respects poses even greater threats

to privacy and civil liberties. Therefore, SECURE IT is not a viable alternative to the Cybersecurity Act. Both bills require substantial amendments to address these concerns.

Sincerely,

American Association of Law Libraries
American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Association of Research Libraries
Hon. Bob Barr
Bill of Rights Defense Committee
Competitive Enterprise Institute
Center for Democracy & Technology
The Center for Media and Democracy
Center for National Security Studies
The Constitution Project
Consumer Federation of America
Cyber Privacy Project
Defending Dissent Foundation
Democrats.com
Doctor Patient Medical Association
Electronic Frontier Foundation
Entertainment Consumers Association
FreedomWorks
Free Press Action Fund
Less Government
Liberty Coalition
National Association of Criminal Defense Lawyers
OpenTheGovernment.org
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Reporters Without Borders
Republican Liberty Caucus
The Rutherford Institute
Remar Sutton - Founder, The Privacy Rights Now Coalition
TechFreedom