June 26, 2014

Chairman Dianne Feinstein
U.S. Senate Select Committee on Intelligence
Washington, DC 20510

Vice Chairman Chambliss
U.S. Senate Select Committee on Intelligence
Washington, DC 20510

Dear Chairman Feinstein, Vice Chairman Chambliss, and Members of the Senate Select Committee on Intelligence:

We the undersigned write to express our grave concerns with the Cybersecurity Information Sharing Act of 2014 (CISA). Over the last year, the public has learned that the National Security Agency (NSA) and other government agencies have significantly stretched the meaning of statutory provisions of law in order to gather sensitive information on hundreds of millions of Americans. The NSA has, without a warrant, searched for the communications of Americans among those collected under laws authorizing surveillance of persons abroad, and engaged in questionable cybersecurity practices, such as compromise of security standards and failure to promptly inform technology companies about security vulnerabilities in their software. CISA ignores these revelations. Instead of reining in NSA surveillance, the bill would facilitate a vast flow of private communications data to the NSA. CISA omits many of the civil liberties protections that were incorporated, after thorough consideration, into the cybersecurity legislation the Senate last considered. For the following reasons, we strongly oppose this legislation and urge against Senate consideration:[1]

- ***Militarization of the Civilian Cybersecurity Program:*** CISA requires that cyberthreat indicators shared from the private sector with the Department of Homeland Security (DHS) be immediately disseminated to the Department of Defense, which includes the NSA and U.S. Cyber Command.[2] This new flow of private communications information to NSA is deeply troubling given the past year's revelations of overbroad NSA surveillance. It would enhance the NSA's role in the civilian cybersecurity program, risking militarization of the program, which would diminish transparency and accountability.
- ***Inadequate Use Limitations:*** CISA's inadequate use limitations risk turning the bill into a backdoor for warrantless use of information the government receives for investigations and prosecutions of crimes unrelated to cybersecurity. CISA permits state, local, and tribal governments to use cyber threat indicators to prevent, investigate, or prosecute *any* crime to which the sharing entity assents.[3] It also allows the Federal Government to use information it receives for an unacceptably broad range of law enforcement purposes, including investigations and prosecutions under the Computer Fraud and Abuse Act (CFAA) and the Espionage Act.[4] Exemption from disclosure law may obstruct transparency regarding law enforcement use of such information. The legislation should contain reasonable use restrictions, similar those in the July 2012 Cybersecurity Act.[5]

---

[1] The concerns posed by this problematic legislation are far- reaching in their effects, and implicate a broad array of issues, including privacy, open government, civil liberties and the integrity of our information technology infrastructure. Many of the undersigned groups share several or all of these concerns as described in today's letter circulated by CDT, which highlights technology and privacy issues with the bill, and a letter organized by the ACLU, which focuses on serious concerns the bill poses for open government, whistleblower protections and civil liberties. These concerns are complementary and overlapping, as evidenced by the significant number of groups signing onto both letters.

[2] Cybersecurity Information Sharing Act of 2014, Sec. 5(c)(1)(C).

[3] Cybersecurity Information Sharing Act of 2014, Sec. 4(d)(4)(A)(i).

[4] Cybersecurity Information Sharing Act of 2014, Sec. 5(d)(5)(A).

[5] S. 3414, Sec. 704(b), 2012.

- ***Failure to Protect Personally Identifiable Information:*** CISA requires private sector entities to remove personal information that pertains to *known* U.S. persons before they share cyber threat indicators. In practice, this will provide little privacy protection because private sector entities will not know the citizenship of the person to whom the information pertains. Further, the bill does not require any effort by the government to remove personal information before sharing cyber threat indicators. Finally, the bill does not require that federal privacy rules be in place before information-sharing begins, increasing the risk of improper dissemination of potentially sensitive personal information.
- ***Overbroad Liability Protection for Countermeasures:*** CISA defines "countermeasure" broadly, and unwisely provides an affirmative defense when a countermeasure causes damage to an entity's network or information system, including actions that would otherwise violate the CFAA, the Wiretap Act, and the Stored Communications Act. This invites reckless and careless use of countermeasures that could inadvertently harm bystanders.
- ***Arbitrarily Harms Average Internet Users:*** The definition of "cybersecurity threat" is overbroad, and includes "any action" that may result in an unauthorized effort to adversely impact the security, confidentiality and availability of an information system or of information stored on such system. Countermeasures can be employed against such threats absent risk of liability. This could lead to use of countermeasures in response to mere terms of service violations. For example, logging into another individual's social networking account – even with their permission – typically violates the website's terms of service, and therefore qualifies as unauthorized access under the CFAA, and could be treated as a "cybersecurity threat." A provision preventing this harm appeared in the July 2012 Cybersecurity Act[6] and should be included in CISA.
- ***Infringing on Net Neutrality Policy:*** Likewise, the July 2012 bill also contained provisions clarifying that nothing in the Act, including overbroad application of the terms "cybersecurity threat" and "countermeasure," could be construed to modify or alter any Open Internet rules adopted by the Federal Communications Commission.[7] Net neutrality is a complex topic and policy on this matter should not be set by cybersecurity legislation.

Cybersecurity legislation intended to protect national security, financial systems, computer users, and the Internet must not undercut essential privacy rights. Accordingly, we urge that these changes be adopted before this legislation moves forward.

Please contact Greg Nojeim, Director of CDT's Project on Freedom, Security & Technology, gnojeim@cdt.org, or Jake Laperruque, CDT's Fellow on Privacy, Surveillance, and Security, jake@cdt.org, regarding any questions.

Thank you for your consideration,

American Civil Liberties Union
American Library Association
Center for Democracy & Technology
Competitive Enterprise Institute
The Constitution Project
Council on Islamic American Relations
Cyber Policy Project
Defending Dissent Foundation

[6] S. 3414, Sec. 708(6)(B), 2012.
[7] S. 3414, Sec. 707(a)(10), 2012.

Demand Progress
DownSizeDC.org, Inc.
The Electronic Frontier Foundation
Free Press Action Fund
FreedomWorks
Government Accountability Project
Liberty Coalition
National Security Counselors
New America Foundation's Open Technology Institute
PEN American Center
People For the American Way
PolitiHacks
R Street
TechFreedom