March 2, 2015

Chairman Richard Burr
Senate Select Committee on Intelligence
United States Senate

Vice Chairman Dianne Feinstein
Senate Select Committee on Intelligence
United States Senate

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

We the undersigned civil society organizations, security experts, and academics write to explain how the Cybersecurity Information Sharing Act of 2015 (CISA),[1] would significantly undermine privacy and civil liberties. We now know that the National Security Agency (NSA) has secretly collected the personal information of millions of users, and the revelation of these programs has created a strong need to rein in, rather than expand, government surveillance. CISA disregards the fact that information sharing can – and to be truly effective, must – offer both security and robust privacy protections. The legislation fails to achieve these critical objectives by including:

- Automatic NSA access to personal information shared with a governmental entity;
- Inadequate protections prior to sharing;
- Dangerous authorization for countermeasures; and
- Overbroad authorization for law enforcement use.

For the following reasons, we urge rejection of CISA in its current form:[2]

***Automatic NSA Access to Personal Information and Communications*:** Since the summer of 2013, NSA surveillance activities, such as the telephony metadata bulk collection program and the PRISM program, have raised nationwide alarm. CISA ignores these objections, and requires real time dissemination to military and intelligence agencies, including the NSA. Congress should be working to limit the NSA's overbroad authorities to conduct surveillance, rather than passing a bill that would increase the NSA's access to personal information and private communications.

Automatic sharing with NSA risks not only privacy, but also effectiveness. During a recent House Intelligence Committee hearing, NSA Director Admiral Mike Rogers stated that sharing threat indicators without filtering out personal data would slow operations and negatively impact NSA's cyber defense activities.[3] Further, in the wake of revelations regarding the PRISM program, major tech companies stated that they would not voluntarily share users' information with the NSA.[4] Automated NSA access could thus disincentivize sharing, undercutting the key goal of the legislation.

***Inadequate Protections Prior to Sharing*:** CISA does not effectively require private entities to strip out information that identifies a specific person prior to sharing cyber threat indicators with the government, a fundamental and important privacy protection.[5] While the bill requires that companies "review" cyber threat indicators for information that identifies a specific person and sometimes remove it, the bill contains no standard to ensure that this review effort is – at a minimum – reasonable.[6]

---

[1] Available at http://images.politico.com/global/2015/03/02/cisa_2015_discussion_draft.html.

[2] Many of us have several other concerns that are not detailed in this letter, including the breadth of the definitions for "cyber threat" and "cyber threat indicator," the blanket authorization for monitoring and complete liability protection for information sharing and monitoring, the absence of any sunsets and the potential scope of the Defense Department's response to cyber attacks contemplated in Section 8(m).

[3] *See*, Rogers, Michael. Statement to the House Permanent Select Committee on Intelligence. *Cybersecurity Threats: The Way Forward*, Hearing, November 20, 2014, *available at* https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf ("[Americans' private data] would be a negative for us. It will lead to a slower sharing of information …. This is not what we want to see. I don't want to see people's personal data").

[4] *See*, Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL issue statements of denial in NSA data mining*, CBS News (June 7, 2013), *available at* http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-ofdenial-in-nsa-data-mining/.

[5] As industry representatives have testified, this requirement would not be onerous or impair ability to effectively share information on cyber threats. *See*, Rep. Adam Schiff et al, *Additional Views* (April 12, 2013) *available at* http://www.scribd.com/doc/135610580/Additional-Views.

[6] Given the lack of standard, a review that is merely cursory would be permissible. CISA Sec. 4(d)(2)(A).

Further, the bill requires companies to remove that information only for individuals that it knows are "not directly related to a cybersecurity threat." This could encourage companies to retain data by default, unnecessarily exposing the information of innocent bystanders and victims to the government, and making it available to law enforcement for a myriad of investigative uses.[7] Legislation should instead require that prior to sharing, companies make at least a reasonable effort to identify all personally identifiable information and, unless it is necessary to counter the cyber threat before sharing any indicators with the government, remove it. The default should be to preserve privacy, rather than to sacrifice it.

***Dangerous Authorization for Countermeasures*:** CISA authorizes countermeasures "notwithstanding any law," including the federal Computer Fraud and Abuse Act. As amended by CISA, federal law would permit companies to retaliate against a perceived threat in a manner that may cause significant harm, and undermine cybersecurity. CISA provides that countermeasures must be "operated on" one's own information systems, but may have off-networks effects – including harmful effects to external systems – so long as the countermeasures do not "intentionally" destroy other entities' systems.[8] Given the risks of misattribution and escalation posed by offensive cyber activities[9] - as well as the potential for misappropriation[10] – this is highly inadvisable. CISA permits companies to recklessly deploy countermeasures that damage networks belonging to innocent bystanders, such as a hospital or emergency responders that attackers use as proxies to hide behind, so long as the deploying company does not *intend* that the countermeasure result in harm.[11] CISA's authorization would not only inadvisably wipe away the Computer Fraud and Abuse Act's current prohibition against these activities, it would be dangerous to internet security.

***Overbroad Law Enforcement Use*:** Law enforcement use of information shared for cybersecurity purposes should be limited to prosecuting specific cyber crimes identified in the bill and preventing imminent loss of life or serious bodily harm. CISA goes far beyond this, and permits law enforcement to use information it receives for investigations and prosecutions of a wide range of crimes involving any level of physical force, including those that involve no threat of death or significant bodily harm, as well as for terrorism investigations, which have served as the basis for overbroad collection programs, and any alleged violations of various provisions of the Espionage Act.[12] The lack of use limitations creates yet another loophole for law enforcement to conduct backdoor searches on Americans – including searches of digital communications that would otherwise require law enforcement to obtain a warrant based on probable cause. This undermines Fourth Amendment protections and constitutional principles.

Cybersecurity legislation should be designed to increase digital hygiene and identify and remediate advanced threats, not create surveillance authorities that would compromise essential privacy rights, and undermine security. Accordingly, we urge that the Committee not approve this bill without addressing these concerns.

Thank you for your consideration,

---

[7] CISA's blanket immunity could, as written, even void private contracts or promises made to users (*e.g.*, in terms of service) to de-identify user information before sharing it with the government.

[8] CISA Sec. 4(b)(1).

[9] *See*, United States. Senate. Committee on Homeland Security and Governmental Affairs. *Hearing on Protecting America From Cyber Attacks: The Importance of Information Sharing*. January 28, 2015. 114th Cong. 1st sess (*statement of Greg Nojeim, Director of the Freedom, Security, and Technology Project, The Center for Democracy & Technology*), 8-9, available at https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/01/HSGAC-Cybersec-tes-1-28-15-final-TEH.pdf.

[10] When certain countermeasures are employed, it is difficult to control "who can intercept the code in transmission, whether it will reach its intended target, whether it will be copied and reused by others, and whether it will spread virally across the internet and cause damage to innocent persons and businesses." *ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media*, 14 (April 4, 2014*), available at* https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf.

[11] CISA, Sec. 4(b)(1).

[12] CISA, Sec. 5(d)(5)(A)(vi).

Civil Society Organizations

Access
American-Arab Anti-Discrimination Committee
American Library Association
Advocacy for Principled Action in Government
American Civil Liberties Union
Association of Research Libraries
Bill of Rights Defense Committee
Brennan Center for Justice
Center for Democracy & Technology
Center for National Security Studies
Competitive Enterprise Institute
Constitutional Alliance
The Constitution Project
Council on American Islamic Relations
Cyber Privacy Project (CPP)
Defending Dissent Foundation
Demand Progress
Electronic Frontier Foundation
Free Press Action Fund
FreedomWorks
Liberty Coalition
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Project on Government Oversight
R Street Institute
Sunlight Foundation

Security Experts and Academics[13]

Ben Adida, Cryptographer
Jacob Appelbaum, The Tor Project
Alvaro Bedoya, Center on Privacy and Technology at Georgetown Law
Brian Behlendorf
David J Farber, University of Pennsylvania
J. Alex Halderman, University of Michigan
Joan Feigenbaum, Yale University
Bryan Ford, Yale University
Matthew D. Green, Johns Hopkins University
Daniel Kahn Gillmor, Technologist
Susan Landau, Worcester Polytechnic Institute
Sascha Meinrath, X-Lab
Peter G, Neumann, SRI International
Ronald L. Rivest, Massachusetts Institute of Technology
Phillip Rogaway, University of California, Davis
Bruce Schneier, Cryptographer and Security Specialist
Christopher Soghoian, Technologist
Eugene H. Spafford, Purdue University
Micah Sherr, Georgetown University
Adam Shostack
Dan S. Wallach, Rice University
Nicholas Weaver, University of California at Berkeley

cc:
Majority Leader Mitch McConnell
Minority Leader Harry Reid

[13] Institutional affiliations are given for identification purposes only; no institutional endorsement is present or implied unless explicitly noted.