June 26, 2014

Majority Leader Harry Reid
United States Senate
Washington, DC 20510

Republican Leader Mitch McConnell
United States Senate
Washington, DC 20510

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

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

Dear Majority Leader Reid, Republican Leader McConnell, Chairman Feinstein and Vice Chairman Chambliss:

We, the undersigned privacy, civil liberties and open government groups, write in strong opposition to the Cybersecurity Information Sharing Act of 2014[1] ("CISA").[*]

Among other things, the bill threatens to create a gaping loophole in existing privacy law that would permit the government to approach private companies; ask for "voluntary" cooperation in sharing sensitive information, including communications content; and then use that information in various law enforcement investigations, including the investigation and prosecution of government whistleblowers under the Espionage Act.

In the year since Edward Snowden revealed the existence of sweeping surveillance programs, authorized in secret and under classified and flawed legal reasoning, Americans have overwhelmingly asked for meaningful privacy reform and a roll back of the surveillance state created since passage of the Patriot Act. This bill would do exactly the opposite. We list select specific concerns below.

Threats to Whistleblowers

- Rather than narrowly limiting the use of information shared to actual "cybersecurity" activity, the bill would permit the government to use the information in the investigation and prosecution of identity theft, terms of service violations and other offenses under the Computer Fraud and Abuse Act, various provisions of the Espionage Act, economic espionage and trade secret violations.[2]

[*] 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.

- Extension of the law to the Espionage Act is particularly troubling.[3] Over the past four years, the Obama administration has aggressively sought to use Espionage Act provisions against government whistleblowers and members of the news media (and, indeed, has brought more "leaks" prosecutions than all other administrations combined).[4] This bill, if misused by administrations current and future, could potentially eliminate due process protections for such investigations, which are already unfairly biased in favor of the prosecution.[5]

Threats to Privacy

- As noted above, nothing in the bill prevents the government from asking companies to "voluntarily" turn over cybersecurity information, broadly defined, and then using that information in criminal proceedings.[6]

- This danger of a potential end-run around the Foreign Intelligence Surveillance Act ("FISA"), the Electronic Communications Privacy Act ("ECPA"), the Fourth Amendment and other crucial privacy protections is compounded by the potentially broad immunity conferred on sharing "in accordance" with the act, and the additional absolute defense when sharing occurs in violation of the act but in "good faith" reliance on the mistaken belief that the sharing is lawful.[7]

- The bill provides that the information, including the content of telephonic or internet communications, is to be transmitted through a portal at the Department of Homeland Security but then shared without any privacy filter and in real-time with the military and the intelligence community, including the National Security Agency.[8] The provision requiring companies to strip out personally-identifiable information ("PII") before sharing only requires them to do so if the information is not "directly related" to a cybersecurity threat, broadly defined—and "cybersecurity threat" is defined broadly enough to potentially include whistleblowers' disclosure of any information their superiors wish to conceal.[9]

- The PII-stripping provision also only mandates sharers do so if they "know" the information belongs to or identifies a "U.S. person," information that many entities will simply not possess.[10]

Threats to Transparency

- Coupled with the broad immunity and good faith defense conferred under § 6, along with the various exemptions from public disclosure through, among other things, the Freedom of Information Act and state sunshine laws,[11] we have serious concern that there is little incentive for entities to expend the resources necessary to adequately protect from inappropriate disclosure PII and other sensitive information about individuals innocent of any wrongdoing.

- The exemptions from disclosure under state and local sunshine laws, and under the federal Freedom of Information Act[12] are unnecessary and would, moreover, deny the public critical information about the government's cybersecurity efforts and about whether the law is being used to circumvent key privacy protections. A key check on government misuse of the proposed

law would be transparency. By contrast, this bill would utterly insulate the government and private sector from public scrutiny and accountability.

In 2012, many of the undersigned groups were successful in achieving a meaningful compromise on cybersecurity legislation that would have protected both privacy and security.[13]

Today, we urge the SSCI to reincorporate these crucial protections, though we note that even with these protections, the bill may continue to pose serious dangers for open government, transparency, whistleblowers, privacy and civil liberties. Specifically, we urge you to:

- Ensure that DHS is the custodian of cybersecurity information voluntarily shared by the private sector, and has the authority to prevent sensitive information from being transmitted to the intelligence community and military without privacy protections;

- Ensure that information shared is "reasonably necessary" to describe a cybersecurity threat;

- Restrict the use of information received under the sharing authority to actual cybersecurity activities, the prosecution of cybercrimes, the protection of individuals from imminent threat of physical harm or death, or to protect children from serious threats;

- Limit FOIA restrictions to those provided by 6 U.S.C. §§ 131-34 (2012).[14]

- Require public disclosure of annual reports from relevant inspectors general describing what information is received, how it is used, who gets it and how it is treated to protect privacy.

- Include a sunset provision in the bill keyed to these reports, which will allow the measure to expire if abuse or misuse is disclosed;

- Allow individuals harmed by inappropriate sharing to sue the government if it intentionally or willfully violates the law.

The law should also make clear that the sharing authority does not permit the government to approach private sector entities with requests for "voluntary" cooperation that would serve to end-run existing privacy protections, including, specifically, ECPA and FISA.

We do not discount the legitimate dangers posed by cyber threats, both from domestic criminals and hostile foreign powers. But, as with all national security authorities, we need not sacrifice crucial civil liberties and privacy safeguards, and especially whistleblower protections, in order to effectively address such dangers. We urge the committee and Congress to carefully reconsider CISA as drafted, and to bring it in line with our law, our Constitution and our national values.

Please do not hesitate to contact Gabe Rottman, legislative counsel and policy advisor at the American Civil Liberties, with any questions. He can be reached at 202-675-2325 or grottman@aclu.org.

Sincerely,

American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Association of Research Libraries
Center for Democracy and Technology
Center for Effective Government
Center for Financial Privacy and Human Rights
Council on American-Islamic Relations
Defending Dissent Foundation
Demand Progress
Electronic Frontier Foundation
FirstAmendment.com
Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project
International Association of Whistleblowers
National Association of Criminal Defense Lawyers
National Coalition Against Censorship
National Latino Farmers and Ranchers Trade Association
National Security Counselors
National Whistleblower Center
New America Foundation's Open Technology Institute
OpenTheGovernment.org
Patient Privacy Rights
People For the American Way
Privacy Times
Project Censored/Media Freedom Foundation
Project On Government Oversight (POGO)
Coleen Rowley
Retired FBI Agent, Apple Valley, MN
Rural Coalition/Coalicion Rural
The Brown Center for Public Policy, Ethics in Business Institute
The Constitution Project
The Sunlight Foundation
The Tully Center for Free Speech at Syracuse University
Whistleblower Support Fund
World Privacy Forum

cc: Senate Committee on the Judiciary Chairman Patrick Leahy and Ranking Member Chuck Grassley, Senate Committee on Homeland Security and Governmental Affairs Chairman Thomas Carper and Ranking Member Tom Coburn, and Senate Select Committee on Intelligence Members

---

[1] All references in this letter are to the discussion draft authored by Senate Select Intelligence Committee ("SSCI") Chairman Dianne Feinstein (D-CA) and Vice Chairman Saxby Chambliss (R-GA) and released earlier this month. *See* Press Release, Sen. Dianne Feinstein, Feinstein Releases Draft Cybersecurity Information Sharing Bill (June 17, 2014), http://1.usa.gov/1jwo5pv.

[2] Once shared, cyber threat indicators ("CTIs") or counter-measure information may be used with the consent of the sharer (private or governmental) for the investigation or prosecution of any state, local or tribal criminal offense, CISA § 4(d)(4), and by the federal government in the investigation and prosecution of offenses under 18 U.S.C. §§ 1028 (identity theft and fraud), 1028A (aggravated identity theft), 1029 (fraud and theft using electronic identifiers), and 1030 (the Computer Fraud and Abuse Act ("CFAA")); and under Chapter 37 (Espionage Act) and Chapter 90 (trade secret theft and economic espionage). Controversially, the CFAA has been used in the prosecution of relatively minor violations of online services' terms of service. *See* Brian Fung, *The Justice Department Used This Law to Pursue Aaron Swartz*, Wash. Post, Feb. 7, 2014, http://wapo.st/1qAKIk5.

[3] For more on the civil liberties implications of the Espionage Act, please see *The Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks*, 112th Cong. (2010) (statement of Laura W. Murphy, Director, Washington Legislative Office ACLU & Michael W. Macleod-Ball, Legislative Chief of Staff and First Amendment Counsel), *available at* http://bit.ly/1mpcCNh.

[4] *See* Leonard Downie Jr. & Sara Rafsky, Comm. to Protect Journalists, The Obama Administration and the Press 1 (Oct. 10, 2013), *available at* http://bit.ly/1cS2cxM ("Six government employees, plus two contractors, including Edward Snowden, have been subjects of felony criminal prosecutions since 2009 under the 1917 Espionage Act . . . compared with a total of three such prosecutions in all previous U.S. administrations."). In one case, the government sought over 30 years' incarceration for a whistleblower who made entirely non-classified disclosures that predated Mr. Snowden's exposure of illegal government surveillance, and revealed billions of dollars of waste in a program that enriched contractors without any effective impact against threats to America's security. This bill creates a back door, all-encompassing loophole to the Whistleblower Protection Enhancement Act and similar legislation covering nearly all government contractors and private sector employees.

[5] *See, e.g.*, Steven Aftergood, *Court Eases Prosecutors' Burden of Proof in Leak Cases*, Fed. of American Scientists, July 29, 2013, http://bit.ly/1lfpN3d.

[6] Specifically, private companies are given broad discretion, "notwithstanding any other provision of law," to transmit CTI information and "countermeasures" to federal, state, local and tribal governments, and to other private entities. CISA § 4(c). CTI is defined to include, among other things, "malicious reconnaissance," broadly defined; "information exfiltrated when it is necessary in order to describe a cybersecurity threat, " which would cover large amounts of communications content; and "any other attribute of a cybersecurity threat." CISA § 2(8).

[7] Put simply, § 6 of CISA provides an entity with discretion to share countermeasures and CTIs, broadly defined, with federal, state, local and tribal governments with little fear of civil or criminal liability under existing privacy law. It thus confers dangerously broad immunity. Specifically, § 6(a) provides complete immunity and automatic dismissal of any claim for monitoring information systems "in accordance with" CISA. Section 6(b) confers complete immunity and automatic dismissal of any claim for the sharing or receipt of CTIs or countermeasures under § 4(c) "in accordance with" CISA and if shared or received consistent with § 5(c), which simply requires initial transmittal to the Department of Homeland Security's intake portal. And, § 6(c) provides that, *even if* a claim is not dismissed or precluded (meaning the claim states a possible violation of CISA), "a good faith reliance by an entity that the conduct complained of was permitted under" CISA will be a complete defense under any claim. Only claims against an entity engaged in gross negligence or willful misconduct will survive dismissal. CISA § 6(d)(1).

[8] CISA § 5(c).

[9] CISA § 4(d)(2). "Cybersecurity threat" is defined as "an action, not protected by the First Amendment . . . , on or through an information system that may result in an unauthorized effort to adversely impact the security,

availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system." CISA § 2(7).

[10] CISA § 4(d)(2).

[11] CISA §§ 4(d)(4)(B), 5(d)(3)(A)-(B).

[12] CISA §§ 4(d)(4)(B), 5(d)(3)(A)-(B), 9.

[13] *See* Michelle Richardson, *New Cybersecurity Amendments Unveiled to Address Privacy Concerns*, ACLU.org, July 19, 2012, http://bit.ly/1uQdcnG.

[14] Critical Infrastructure Information Act, Pub. L. No. 107-296, 116 Stat. 2150 (2002) ("CIIA"). CIIA already provides protection from disclosure for voluntarily shared critical infrastructure information, subject to certain conditions, and would cover CTIs and counter-measure information where an exemption is warranted.