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:

The undersigned open government and civil liberties groups write in strong opposition to the Cybersecurity Information Sharing Act of 2015 ("CISA"). In our view, the bill does far more to increase surveillance and undermine transparency than to protect against cyber threats.

The draft bill[1] would increase the intelligence community's access to Americans' personal information without adequate legal protections against the use of "cyber-threat" information to investigate whistleblowers or conduct broad surveillance unrelated to specific cybersecurity threats. It would also add a new and unnecessary exemption to the Freedom of Information Act (FOIA), which has been a pillar of government transparency in an age of increasing government secrecy.

Section 5(d)(5)(A) of the draft bill, entitled "Disclosure Retention, and Use", permits the federal government to use so-called "cyber-threat indicators" it receives from private companies for a wide variety of law enforcement purposes, including:

- Investigating violations of the Espionage Act, the Computer Fraud and Abuse Act, and a wide variety of other federal crimes.[2]

  The authorization to use cyber-threat information in Espionage Act investigations is particularly worrisome in light of the increasing use of the Espionage Act to justify surveillance of journalists and their sources, and criminal prosecution of sources. This provision, when combined with CISA's overly broad definitions of "cybersecurity threat," "cyber threat indicator," "security control," and "security vulnerability"[3] and its weak requirements for removing personal information,[4]

[1] The letter refers to the draft version of CISA published at http://images.politico.com/global/2015/03/02/cisa_2015_discussion_draft.html.
[2] CISA draft, § 5(d)(5)(A)(vi).
[3] CISA draft, § 2.

could be used to justify searches of journalists' communications with sources and whistleblowers' communications with Congress.

- "responding to, or otherwise preventing or mitigating, a terrorist act" even if there is no imminent threat of death or bodily harm, or investigating any terrorism-related crime.[5]

  In 2013, we learned that section 215 of the PATRIOT Act, which allows the FBI to request production of specific "tangible things" for "an investigation to protect against international terrorism or clandestine intelligence activities," had been interpreted to authorize bulk collection of virtually all Americans' telephone call detail records. The government argued that it needed to "collect it all" to find and isolate terrorists' communications. The intelligence community could use the same rationale—that it is necessary to collect everyone's information, of any type, and all the time, in order to prevent acts of terrorism—to store and search information provided under CISA.

Section 10 of the bill, entitled "conforming amendments," significantly modifies the Freedom of Information Act (FOIA) by creating a new exemption to authorize the government to withhold any "information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2015."[6] This "technical amendment" would be the most far-reaching substantive broadening of the Act's exemptions—thus broadly weakening FOIA as a whole—since 1986.

Amendments to FOIA, particularly the addition of an entirely separate exemption, should not be enacted without careful consideration by the Senate Judiciary Committee, which has jurisdiction over FOIA. Careful consideration by that Committee of FOIA-related legislation, including public hearings, is necessary to ensure that the bill promotes transparency and public accountability while allowing the government to withhold only that information which truly requires protection. Time and again over the past quarter-century, proposals to amend the Act's existing exemptions have been rejected as unwise.

It is important to note that most, if not all, of the sensitive information the draft bill specifies needs protection is already protected from disclosure under the FOIA. Section 5(d)(2) and (3)(A) and (B)of the draft bill, entitled "Disclosure Retention, and Use" note – and reiterate – existing protections for such shared information. Under (2) PROPRIETARY INFORMATION.—"A cyber threat indicator or countermeasure provided by an entity to the Federal Government under this Act shall be considered the commercial, financial, and

---

[4] CISA draft, § 4(d)(2).
[5] CISA draft, § 5(d)(5)(A)(iv)
[6] CISA draft, § 10(a).

proprietary information of such entity when so designated by such entity;" and (3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and countermeasures provided to the Federal Government under this Act shall be—(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records. These are existing statutory exemptions to the Freedom of Information Act; "voluntarily shared information" has been protected as Critical Infrastructure Information since 2001. Yet, even with these existing protections, the bill would create a new non-discretionary (b)(3) exemption for all such information in addition to the new exemption in Section 10.

We urge you to reject CISA in its entirety. This Cyber Intelligence Surveillance Act is not only overbroad and duplicative; it also actively erodes statutory protections that citizens and open-government groups have consistently relied on. We look forward to working with Congress to ensure any true cybersecurity legislation passed into law protects both our nation's computer networks and our civil liberties, while preserving and promoting transparency and accountability to the public. If you would like to discuss these issues further, please contact Patrice McDermott, Executive Director of OpenTheGovernment.org, at 202-332-6736 or pmcdermott@openthegovernment.org.

Sincerely,

American Civil Liberties Union
Cause of Action
Citizens for Ethics and Responsibility in Washington (CREW)
Defending Dissent Foundation
Government Accountability Project
OpenTheGovernment.org
Project on Government Oversight (POGO)
Public Record Media
R Street Institute
Society of Professional Journalists
The Sunlight Foundation

Cc: Senator Chuck Grassley, Chairman, Senate Judiciary Committee; Senator Patrick Leahy, Ranking Member, Senate Judiciary Committee; Senator John Cornyn