Dear Senator,

The undersigned open government and civil liberties groups write in strong opposition to the Cybersecurity Information Sharing Act of 2015, S. 754 ("CISA"). In our view, the bill does far more to increase surveillance and undermine transparency than to protect against cyber threats.

The bill reported out of the Senate Intelligence Committee 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.[1]

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"[2] and its weak requirements for removing personal information,[3] could be used to justify searches of journalists' communications with sources and whistleblowers' communications with Congress and the Senate.

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."[4] 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. It would also be the first new exemption to FOIA itself since the 1960s. 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.

---

[1] CISA, § 5(d)(5)(A)(vi).
[2] CISA, § 2.
[3] CISA, § 4(d)(2).
[4] CISA, § 10(a).

Both the House Intelligence Committee and House Homeland Security Committee stripped out the blanket exemption 10 from, respectively, and the National Cybersecurity Protection Advancement Act ("NCPAA")[5] and the Protection Cyber Network Act ("PNCA")[6] passed in the House in April. House Intelligence Committee Chairman Devin Nunes introduced an amendment to strip the exemption in order to remove a direct amendment to the FOIA, and emphasized that the NCPAA already contained a "strong exemption of cyber threat information and defensive measures from disclosure," and added that removing the exemption 10 did not "have a substantive effect on the exemption of cyber threat information from disclosure laws."[7] Nonetheless, the blanket exemption 10 still remains in the CISA currently pending before the Senate.

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 existing law. 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. In addition to affirming these existing prohibitions, the bill would create a new non-discretionary (b)(3) exemption for all such information. We believe that the new (b)(3) exemption is itself redundant and unnecessary; adding a new FOIA exemption *and* a (b)(3) exemption is doubly so.

Despite this redundancy, the new FOIA exemption could set a dangerous precedent for further amendments to FOIA by the Senate Select Committee on Intelligence (SSCI). For example, if CISA is signed into law, the intelligence committee could add even more exemptions to FOIA by drafting them as amendments to CISA without adequate notice to the Judiciary Committee. SSCI lacks expertise on Freedom of Information Act issues, is extremely deferential to intelligence community requests for secrecy, and closes virtually all committee hearings and markups to the public. These practices are directly at odds with FOIA's goals.

The problems with CISA, however, are broader than its unwise and unnecessary FOIA provisions. 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 urge you to reject CISA in its entirety. We look forward to working with the Senate 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.

---

[5] H.R. 1731, 114th Cong. (2015).
[6] H.R. 1560, 114th Cong. (2015).
[7] Congressional Record Volume 161, Number 59, April 22, 2015, House, Pages H2381-H2398; http://origin.www.gpo.gov/fdsys/pkg/CREC-2015-04-22/html/CREC-2015-04-22-pt1-PgH2381-3.htm.

Sincerely,

Advocacy for Principled Action in Government
American Association of Law Libraries
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