WASHINGTON
LEGISLATIVE OFFICE

August 4, 2015

RE: Oppose S. 754, the Cybersecurity Information Sharing Act of 2015

Dear Senator,

On behalf of the American Civil Liberties Union, please find attached our vote recommendation for S. 754, the Cybersecurity Information Sharing Act of 2015 ("CISA"). We strongly urge you to vote NO on CISA, a bill that would expand warrantless government surveillance and harm the privacy rights of all Americans. While the manager's amendment made some improvements to the bill, significant concerns remain. These include:

- Granting private companies broad immunity from legal liability when they share private customer information with the government for a "cybersecurity purpose," without adequate protections to ensure they remove personally identifiable information.
- Requiring that information shared with the government be automatically forwarded to numerous agencies, including the FBI and NSA, which could then use the shared information in investigations and prosecutions that have nothing to do with cybersecurity, including in investigations of members of the press who report on classified information.

Furthermore, because CISA would result in government agencies receiving and storing a large amount of sensitive personal information, it puts Americans at even greater risk online by making the U.S. government an even more desirable target for hackers and foreign spies. Technologists have roundly criticized CISA for this reason.[1] And a July 31, 2015 letter from the Department of Homeland Security also states that CISA will make tracking cyber threats *more* difficult.[2]

CISA is a surveillance bill that harms privacy and security. **We urge you to vote NO on CISA.**

Please call Legislative Counsel/Policy Advisor Gabe Rottman with any questions at (202) 675-2325.

Best Regards,

Michael W. Macleod-Ball
Acting Director

Gabriel Rottman
Legislative Counsel/Policy Advisor

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] Letter from Technologists to Sen. Feinstein, Sen. Burr, Rep. Schiff, Rep. Nunez, and Rep. McCaul. (April 16, 2015), *available at*, http://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf.
[2] Letter from Alejandro N. Mayorkas, Deputy Secretary, U.S. Department of Homeland Security, to Sen. Al Franken (July 31, 2015), *available at* http://www.franken.senate.gov/files/documents/150731DHSresponse.pdf.

ACLU Vote Recommendation for S. 754, the Cybersecurity Information Sharing Act of 2015

The American Civil Liberties Union recommends a NO vote on S. 754, the Cybersecurity Information Sharing Act of 2015.

Under CISA, a company will be able to share "cyber threat indicators," a term broadly defined to allow the sharing of private information and communications, with the government. The sharing would be exempt from all privacy laws and laws requiring warrants or subpoenas for the production of electronic communications, and companies would enjoy broad legal immunity when sharing for "cybersecurity purposes," which could result in the oversharing of personal information.

- There is no requirement to strip out all personally identifiable information (PII) from the shared information. The company must only remove PII if it "knows" at the time of sharing that the information is not "directly related" to a cybersecurity threat. (Sec. 4(d)(2)).

Information shared by companies would be automatically forwarded to the FBI and NSA for use in prosecutions and investigations unrelated to cybersecurity.

- The Department of Homeland Security must disseminate all threat indicators it receives in an "automated manner" that is "not subject to delay [or] modification." CISA would not allow DHS to strip out improperly shared information or PII before forwarding to other agencies. (Sec. 5(a)(3)(ii)).
- Information received by the government could be used in investigations and prosecutions of crimes having nothing to do with cybersecurity, including Espionage Act investigations, which have repeatedly targeted whistleblowers and investigative journalists. (Sec. 5(d)(5)(A)).

CISA is a surveillance bill. Its provisions would make it easier for the government to obtain, retain and use personal information and private communications for purposes that go well beyond cybersecurity without any of the standards or safeguards typically required under the Constitution. Furthermore, CISA would put consumers' data at more risk by creating an even greater incentive for hackers to target federal agencies and would make it harder for DHS to effectively track real cyber threats. We urge the Senate to vote NO on S. 754.

Please call Legislative Counsel/Policy Advisor Gabe Rottman with any questions at (202) 675-2325 or at grottman@aclu.org.