WASHINGTON
LEGISLATIVE OFFICE

April 16, 2012

Re: ACLU Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011 (CISPA)

Dear Representative,

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

LAURA W. MURPHY
DIRECTOR

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

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

On behalf of the American Civil Liberties Union, a non-partisan organization with over half a million members, countless additional activists and supporters, and 53 affiliates nationwide, we write in opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011 (CISPA), expected to be considered by the full House next week Even with the amendments accepted by the Intelligence Committee at markup, and the amendments now posted in the discussion draft[1] on the Intelligence Committee's website, CISPA would violate Americans' privacy by permitting companies to share vast amounts of personal information with the government in the name of cybersecurity with little meaningful oversight. We urge you to vote 'NO' when this bill comes to the House floor for consideration.

The Cyber Intelligence Sharing and Protection Act would create a cybersecurity exception to all privacy laws and allow companies to share the private and personal data they hold on their American customers with the government for cybersecurity purposes. The bill would not limit the companies to sharing only technical, non-personal data. Instead, it would give the companies discretion to decide the type and amount of information to turn over to the government, and permit them to share the information with the government agency of their choice, including military agencies like the National Security Agency. These entities would receive liability protection under CISPA and would be immune from criminal or civil liability, even after an egregious breach of privacy. Further, once an individual's information is shared with the government, there would be little restriction on the use of that information. It could be used for any purpose

[1] The comments in this letter reflect the amendments accepted by the House Permanent Select Committee on Intelligence at its December 1, 2011 markup and the potential floor amendments posted on the HPSCI website at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/DiscussionDraftHR3523.pdf, last accessed on April 16, 2012.

whatsoever as long as a significant purpose relates to cybersecurity or protection of national security.

Beyond the potential for massive data collection authorization, the bill would provide little meaningful oversight of, or accountability for, the use of these new information-sharing authorities. No federal agency or official has been tasked with issuing explicit guidance to companies and government agencies as to how best protect privacy, and there are no consequences for violating the limited restrictions currently in the bill. While the bill now contains important language requiring an annual audit by the Intelligence Inspector General, the oversight provisions in total are not robust enough to balance out the extraordinary potential for abuse under this new program.

Writing a statute to govern the sharing of cybersecurity information is a complex and challenging task. But any new programs simply must respect privacy, and the three other information sharing proposals in the House and Senate, authored by both Democrats and Republicans, offer more protections for Americans' rights than CISPA. Even the current information sharing program run by the Department of Homeland Security includes more explicit and rigorous protections, making CISPA a step backwards from current practice. The House can borrow from any one of these programs or bills in building a program that better respects privacy.

Any new information-sharing legislation must at a minimum do the following:

- Narrowly define the privacy laws it will contravene. Congress must carefully consider which specific privacy laws truly inhibit necessary information-sharing and craft narrow exceptions limited to just those critical circumstances.

- House domestic cybersecurity efforts in a civilian agency. Congress must not empower military or intelligence agencies such as the National Security Agency to collect the internet usage data of Americans. Cybersecurity efforts on American soil should be led by the private sector, and any government information collection must be coordinated by a civilian government agency.

- Require companies to remove personally identifiable information (PII) from data they share with the government. While sharing technical data can take place without implicating civil liberties, a presumption of privacy should protect PII. Sharing PII should be an exception and not the norm, even if there could be certain limited exceptions to cover legitimate emergencies or other narrowly defined situations.

- Limit government use of information shared for cybersecurity purposes. Cybersecurity information-sharing should not become a windfall of data for the federal government to use as it pleases. Any information shared with the government must have strict use limitations to ensure that this new program doesn't become an end run around privacy laws that would otherwise offer stronger protections.

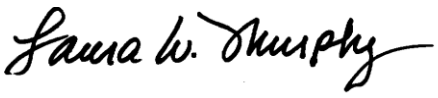
- Create an oversight and accountability structure that includes public and congressional reporting. The executive branch must provide regular, substantive and public reporting, ideally

by multiple Inspectors General and/or privacy officers. There must also be accountability for those who overshare or misuse sensitive information.

Because CISPA does not include any such provisions, we urge a 'NO' vote when it comes to the House floor for a vote.

We appreciate your consideration and have enclosed an interested persons memo that discusses information sharing and all the pending legislative proposals in more detail. Please contact Michelle Richardson, Legislative Counsel, should you need more information.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office

Michelle Richardson
Legislative Counsel

Enclosure: Interested Persons Memo