Speaker Paul Ryan
United States House of Representatives

Democratic Leader Nancy Pelosi
United States House of Representatives

Majority Leader Kevin McCarthy
United States House of Representatives

Majority Leader Mitch McConnell
United States Senate

Minority Leader Harry Reid
United States Senate

December 7, 2015

Dear President Barack Obama and Members of Congress,

The undersigned organizations urge you to oppose the newly negotiated "conference" legislation that purports to resolve differences between H.R. 1560, which includes both the Protecting Cyber Networks Act (PCNA) and the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), and the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754). The current version of these bills is the result of secret negotiations between the House and Senate intelligence committees at the expense of critical expert input from the House Committee on Homeland Security, and it loses any advantages and improvements in the Homeland Security Committee's own cybersecurity bill, the NCPAA.

Many organizations and companies[†] opposed CISA in its earlier form because they believed it would damage Americans' privacy without improving security. Civil liberties organizations' concerns are well known. Companies share many of the same concerns. But companies also work hard to earn users' trust when it comes to privacy. Without that trust, business suffers. Instead of addressing these concerns with the existing bills, the current proposal would build a government regime that makes it impossible for companies to guarantee the protection of customers' civil liberties and privacy, while also failing to meaningfully improve cybersecurity.

Specifically, the text just negotiated is publicly reported to include the following gravely flawed changes to the passed bills. These changes would render it an unacceptably compromised piece of legislation that will be both unhelpful for cybersecurity and dangerous to Americans' civil liberties. Specifically, It threatens to:

- Create a loophole that would allow the President to remove the Department of Homeland Security, a civilian agency, as the lead government entity managing information sharing;
- Reduce privacy protections for Americans' personal information;
- Overexpand the term "cyber threat" to facilitate the prosecution of crimes unrelated to cybersecurity;
- Expand already broad liability protection for information disclosure;

[†] The following technology companies and industry associations previously have expressed grave concerns about CISA: Apple, Automattic, Business Software Alliance, Computer and Communications Industry Association, Dropbox, Google, LinkedIn, reddit, Salesforce, Twilio, Twitter, Wikipedia, Yahoo, and Yelp.

- Preempt state, local or tribal disclosure laws on any cyberthreat information shared by or with a State, tribal, or local government; and
- Eliminate a directive to ensure data integrity.

Moreover, these modifications worsen bills that already contained fundamental flaws. These bills, in particular CISA, would already:

- Dramatically expand the amount of sensitive information held by government agencies with dismal records on data security;
- Undermine civilian agency leadership of cybersecurity efforts;
- Institute blind, automatic transfer of personal information to intelligence agencies, including the National Security Agency, that would be authorized to use the information for non-cybersecurity purposes;
- Allow private entities to transfer irrelevant and sensitive personally identifiable information to the government without accountability;
- Allow companies and other entities to use “defensive measures” to protect "information systems," which could unintentionally harm systems and computers of innocent parties; and
- Provide unnecessarily expansive liability protections to companies, thereby undermining customer trust and limiting judicial remedies for those whose rights are violated.

Because it fails to resolve these weaknesses originally present within the three bills and makes new and alarming changes to them, we strongly object to the intelligence committee’s latest iteration of “cybersecurity” legislation and the undemocratic process that produced it.

Please join us in rejecting these new, troubling flaws and insisting that any version of cybersecurity legislation brought to the floor of either chamber draws heavily upon NCPAA and the expertise and extensive input of the House Committee on Homeland Security.

Sincerely,

Advocacy for Principled Action in Government
Amicus
American Library Association
Bill of Rights Defense Committee
Campaign for Liberty
Constitutional Alliance
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.
Fight for the Future
Free Press Action Fund
FreedomWorks

Media Alliance
Niskanen Center
OpenMedia
OpenTheGovernment.org
Restore the Fourth
R-Street Institute
X-Lab

CC:

Chairman Michael McCaul
Homeland Security Committee

Ranking Member Bennie Thompson
Homeland Security Committee

Chairman Ron Johnson
Committee on Homeland Security and Governmental Affairs and

Ranking Member Thomas R. Carper
Committee on Homeland Security and Governmental Affairs

Chairman Devin Nunes
House Permanent Select Committee on Intelligence

Ranking Member Adam Schiff
House Permanent Select Committee on Intelligence

Chairman Richard Burr
Senate Select Committee on Intelligence

Vice Chairman Dianne Feinstein
Senate Select Committee on Intelligence