December 17, 2015

Dear Member of Congress:

We, the undersigned civil society organizations and security experts write to urge opposition to the Cybersecurity Act of 2015, formerly called the Cybersecurity Information Sharing Act (CISA, S. 754)[1], if it comes to the House floor for a vote. We strongly oppose its inclusion in Division N of the omnibus funding package. This bill seriously threatens privacy, civil liberties, and government accountability, and would undermine cybersecurity, rather than enhance it. As such, it should be debated pursuant to regular process, and members should have the opportunity to record their votes on this highly controversial bill.

As passed in the Senate, CISA raised such serious privacy and security concerns that trade associations including the BSA The Software Alliance, the Computer & Communications Industry Association (CCIA), and major technology companies like Apple and SalesForce, as well as many others, vocally opposed the legislation.[2] The Cybersecurity Act of 2015 is a renamed version of CISA that fails to address core privacy concerns, while weakening the marginal privacy protections that were previously included in the bill.

This new bill would significantly increase the National Security Agency's (NSA) and the Federal Bureau of Investigation's (FBI) access to personal information, and authorize the federal government to use that information for a myriad of purposes unrelated to cybersecurity. It also fails to provide strong privacy protections or adequate clarity about what actions can be taken, what information can be shared, and how that information may be used by the government.

We strongly oppose this information sharing bill because it would:[3]

- **Authorize companies to significantly expand monitoring of their users' online activities, and permit sharing of vaguely defined "cyber threat indicators" without adequate privacy protections prior to sharing:[4]** This could result in the unnecessary scrutiny of innocent Internet users' online activities, and the sharing of their personal information, as well as information about that Internet use, including content of their online communications. Sponsors of the bill watered down the requirement for companies to remove personal information from the standards that were included in the House-passed bills. The current bill includes a standard that would allow companies to default to sharing personal information not necessary to describe a cyber threat, rather than removing it, and requires only that companies engage in a cursory review of indicators to identify personal information. This weak protection poses a threat to privacy, as well as to data security, as hackers and nation-state actors often seek out and steal personally identifiable information when they breach company and government networks.

- **Require federal entities to automatically disseminate to the NSA all cyber threat indicators they receive, including personal information about individuals:** This fails to effectively cement civilian control of domestic cybersecurity information sharing and could vastly increase the NSA's access to Americans' information.

[1] Many of the undersigned groups have signed letters strongly opposing CISA and PCNA for many of the same reasons detailed in this letter. *See* Coalition Letter Opposing CISA as Reported Out of Committee (April 20, 2015), http://bit.ly/1D82Mmw; *and* Coalition Letter Opposing PCNA (April 20, 2015), http://bit.ly/1Hbqwhf.

[2] Robyn Greene, *Tech industry leaders oppose CISA as dangerous to privacy and security,* The Hill, Oct. 21, 2015, http://thehill.com/blogs/pundits-blog/technology/257601-tech-industry-leaders-oppose-cisa-as-dangerous-to-privacy-and.

[3] Many of us have several other concerns that are not detailed in this letter, including the breadth of the definitions for "cyber threat," and "cyber threat indicator," which would allow companies to share information that describes mere attributes of threats. Additional concerns include the scope of the liability protection for information sharing and monitoring, which could lead to over-sharing; and the unnecessary and expansive requirement that cyber threat indicators and defensive measures shared pursuant this bill would be exempt under the Freedom of Information Act (5 U.S.C. 552(b)).

[4] Current law already permits companies to monitor their networks to protect their own rights and property and bill proponents have not explained why vast new monitoring authority is needed. The bill goes far beyond granting authority to monitor for advanced persistent threats that could pose a risk to specific information systems of third parties.

- **Allow Companies to Share Information Directly with the NSA or FBI:** The bill would authorize companies to share information with any federal entity, including law enforcement and intelligence agencies like the NSA and FBI, notwithstanding any other provision of law. Companies would only get additional liability protections for sharing through an authorized portal, which would initially be at the Department of Homeland Security (DHS).

- **Allow the president to establish the Office of the Director of National Intelligence (DNI), the FBI, and any other appropriate civilian federal entity as a portal through which companies may share information with liability protection:** This undermines efforts to ensure that the cybersecurity program does not undermine protections afforded to law enforcement surveillance and could also weaken cybersecurity by increasing the likelihood that DHS would never see cyber threat information essential to its cybersecurity mission.[5]

- **Authorize overbroad law enforcement uses that go far outside the scope of cybersecurity:** Law enforcement would be allowed to use cyber threat indicators to investigate and prosecute crimes and activities that have nothing to do with cybersecurity, such as threat of serious bodily injury or death, terrorism, or serious economic harm, regardless of whether the harm is imminent. There is a requirement that there be a "specific threat," but the bill fails to define that term, and intelligence agencies such as the NSA or FBI could interpret it in such a broad manner that they would take it as license to continually mine the cyber threat indicators they receive for information to be used in unrelated criminal investigations. Additional concerning use authorizations include investigations under the Espionage Act, which could result in even more aggressive crackdowns against national security journalists and their sources, and retaliation against government whistleblowers; and investigations into identity theft and trade secret violations. The use authorizations included in this bill undermine traditional due process protections, and turn it into a cyber-surveillance bill rather than a cybersecurity bill; and

- **Authorize Companies to engage in problematic defensive measures:** The bill would provide a sweeping authorization for companies to engage in defensive measures, previously referred to as countermeasures. Companies already legally engage in a range of activities to protect their systems and the information that resides on or transits their systems, so it is unclear why Congress should authorize companies to deploy vaguely defined defensive measures "notwithstanding any other provision of law."

The Cybersecurity Act of 2015, formerly called CISA, fails to effectively cement civilian control of domestic cybersecurity information sharing, threatens privacy and civil liberties, and could harm cybersecurity and data security. **We urge you to oppose the bill and its inclusion in the omnibus funding package. We further urge you to vote "No" on the bill if it comes to the floor for an independent vote.**

Thank you for your consideration.

Sincerely,

Civil Society Organizations

Access Now
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Amicus
Arab American Institute
Bill of Rights Defense Committee
Brennan Center for Justice

[5] Alejando N. Mayorkas, Deputy Sec., Dept. of Homeland Sec., Letter to Sen. Al Franken concerning the Cybersecurity Information Sharing Act of 2015 (July 31, 2015), http://www.franken.senate.gov/files/documents/150731DHSresponse.pdf.

Campaign for Liberty
Center for Democracy & Technology
Constitutional Alliance
The Constitution Project
The Copia Institute
Defending Dissent Foundation
Demand Progress
Electronic Frontier Foundation
Fight for the Future
Freedom of the Press Foundation
FreedomWorks
Free Press Action Fund
Government Accountability Project
Hackers/Founders
Human Rights Watch
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Niskanen Center
OpenMedia
OpenTheGovernment.org
PEN American Center
Privacy Rights Clearinghouse
Restore the Fourth
R Street
Venture Politics
X-Lab

Security Experts and Academics

Sergey Bratus, Research Associate Professor, Dartmouth College.
Eric Brunner-Williams, retired
John Covici, Systems Administrator, Covici Computer Systems
Prof. David L. Dill, Stanford University
Riley Eller, Inventor and Security Strategist; Chief Technology Officer, CoCo Communications
Robert G. Ferrell, Special Agent, Information Security (Ret.), U.S. Dept. of Defense
Dr. Richard Forno, Jr. Affiliate Scholar, Stanford Center for Internet and Society*
Joe Grand, Principal Engineer and Security Researcher, Grand Idea Studio, Inc.
Carl Hewitt, Board Chair, Standard IoT Foundation
Richard S. Kulawiec, Senior Internet Security Architect, Fire on the Mountain, LLC
Ryan Lackey, Security Product Strategy at CloudFlare*
Christopher Liljenstolpe, Co-Chair IETF OpenPGP working group & Internet infrastructure architect*
Morgan Marquis-Boire - Citizen Lab, Munk School of Global Affairs, University of Toronto
Peter G. Neumann, Senior Principal Scientist, SRI International, Computer Science Lab, Moderator of the ACM Risks Forum*
Benjamin C. Pierce, Henry Salvatori Professor of Computer and Information Science
Lauren Weinstein, Co-Founder, People For Internet Responsibility

*Associations are for informational purposes only