April 20, 2015

Dear Senator:

We the undersigned civil society organizations, security experts, and academics write to urge opposition to the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754)[1] when it comes to the Senate floor for a vote. CISA would seriously threaten privacy and civil liberties, and could undermine cybersecurity, rather than enhance it.

CISA would significantly increase the National Security Agency's (NSA) access to personal information, and authorize the federal government to use that information for a myriad of purposes unrelated to cybersecurity. The revelations of the past two years concerning the intelligence community's abuses of surveillance authorities and the scope of its collection and use of individuals' information demonstrates the potential for government overreach, particularly when statutory language is broad or ambiguous. Notably, Congress has yet to enact reforms that would effectively rein in the government's activities.

CISA fails to provide both strong privacy protections and adequate clarity about what actions can be taken, what information can be shared, and how that information may be used by the government. CISA:

- Authorizes sharing of vaguely defined "cyber threat indicators" without adequate privacy protections prior to sharing;
- Permits companies to share cyber threat indicators, which may include information about innocent individuals, directly with the NSA;
- Requires that federal entities automatically disseminate to the NSA all cyber threat indicators they receive, including personal information about individuals;
- Authorizes overbroad law enforcement uses that go far outside the scope of cybersecurity; and
- Authorizes companies to deploy dangerous countermeasures, euphemistically called "defensive measures," that could damage data and computer systems of innocent third parties who did not perpetrate the threat.

We strongly urge you to oppose CISA for the following reasons:[2]

Authorization to Share Vaguely Defined "Cyber Threat Indicators" and Inadequate Privacy Protections Prior to Sharing: CISA could authorize vast amounts of personal data to be shared with the government, even when it is not necessary to identify or respond to a cybersecurity threat, because of its overbroad authorizations, vague definitions, and weak privacy requirements.

---

[1] Cybersecurity Information Sharing Act of 2015 (CISA, S. 754), https://www.congress.gov/114/bills/s754/BILLS-114s754pcs.pdf.

[2] 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; the absence of a sunset; the creation of the first new exemption to the Freedom of Information Act (5 U.S.C. 552(b)) since it was passed in 1966 (though current exemptions have been amended); and the potential scope of the Department of Defense's response to cyber attacks contemplated in Section 8(m).

CISA authorizes companies to monitor Internet users' activities in order to identify a cybersecurity threat to any entity anywhere, even if such monitoring would otherwise be illegal under a privacy law.[3] CISA's sponsors have not explained why such a broad new authorization is necessary. Under current law, companies may already monitor their networks to identify threats to their own rights and property and share information about those threats with other entities. CISA then authorizes companies to share cyber threat indicators derived from that expanded monitoring with the government, as well as with other companies.[4]

While the bill requires companies to remove some personal information before sharing it with the government, that requirement is weak. CISA permits companies to leave personal and identifying information in indicators it shares with the government unless the company knows that the information is not directly related to a threat.[5] This allows companies to share virtually all personal and identifying information in indicators by default.

Permission To Share Personal Information In Indicators with the NSA: CISA pre-empts all law and enables companies that operate in the civilian sector to share cyber threat indicators with any agency of the federal government. Though liability protection would attach only to sharing with the government through the Department of Homeland Security (DHS), permission to share notwithstanding any law is much broader. This undermines privacy and the development of civilian expertise and control of the government's cybersecurity program for the civilian sector.

Requirement that All Indicators Shared With Federal Government be Automatically Disseminated to the NSA, Including Personal Information of Individuals: CISA fails to effectively cement civilian control of domestic cybersecurity information sharing. It requires that the government recipient of any cyber threat indicator automatically disseminate that indicator to the Department of Defense and the NSA, and to non-military intelligence agencies. Additionally, the receiving entity is prohibited from modifying the indicator prior to dissemination, which may prevent that entity from reviewing the indicator for and removing personal or identifying information that is unnecessary to identify or respond to a cyber threat.[6] This could vastly and unnecessarily increase the NSA's access to innocent users' information.

Authorization for Federal, State, and Local Governments to Use Indicators for Criminal Investigations That Are Completely Unrelated to Cybersecurity: CISA authorizes federal, state, and local governments to use cyber threat indicators to investigate crimes that have nothing to do with cybersecurity, such as robbery, arson, and carjacking, as well as identity theft and trade secret violations. While these crimes are serious, they should not be exempt from long-standing due process protections. CISA would also permit the use of sensitive personal information in 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.[7] This threat is amplified by the significant amount of personal and identifiable information that could be shared under CISA.

Authorization to Deploy Dangerous Defensive Measures: CISA authorizes companies to deploy "defensive measures" (also commonly referred to as "countermeasures") on their systems to

[3] CISA, Sec. 4(a).
[4] CISA, Sec. 4(c).
[5] CISA, Sec. 4(d).
[6] CISA, Sec. 5(a)(3).
[7] CISA, Sec. 5(d)(5)(A), and CISA Sec. 4(d)(4)(A).

retaliate against perceived cybersecurity threats, even when the countermeasure would be otherwise illegal under the Computer Fraud and Abuse Act.[8] CISA's current authorization is more limited than previous iterations, but it would still threaten Internet security rather than enhance it.

CISA authorizes the negligent use of defensive measures that could cause significant, though not substantial harm to a third party's information system. Additionally, it does not prohibit defensive measures from causing harm to devices that may be connected to a third party's information system.[9] These impacts could be far-reaching in light of how interconnected networks have become, and the expansion of that interconnection through the "Internet of things." We urge against any new and unnecessary authorization for defensive measures or countermeasures, especially since it is impossible to guarantee that the effects of defensive measures will be limited to one's own system.

CISA's overbroad monitoring, information sharing, and use authorizations effectively increase cyber-surveillance, while the authorization for the use of defensive measures may actually undermine cybersecurity. We urge you to oppose CISA.

Thank you for your consideration.

Sincerely,

CIVIL SOCIETY ORGANIZATIONS

Access
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Association of Research Libraries
Bill of Rights Defense Committee
Brennan Center for Justice
Center for Democracy & Technology
Center for National Security Studies
Constitutional Alliance
The Constitution Project
Council on American-Islamic Relations
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org
Electronic Frontier Foundation
Fight for the Future
Freedom of the Press Foundation
FreedomWorks
Free Press Action Fund
Government Accountability Project
Hackers/Founders

[8] CISA, Sec. 4(b).
[9] CISA, Sec. 2(7).

Human Rights Watch
Liberty Coalition
Media Alliance
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
OpenTheGovernment.org
PEN American Center
Restore the Fourth
R Street
Student Net Alliance
Venture Politics
X-Lab

SECURTY EXPERTS AND ACADEMICS:

Jacob Appelbaum, Security and privacy researcher, The Tor Project
Brian Behlendorf, Technologist
Jon Callas, Cryptographer and Inventor
Antonios A. Chariton, Security Researcher, Institute of Computer Science, Foundation of Research and Technology -- Hellas
Rik Farrow, Editor, USENIX
Dr. Richard Forno, Jr. Affiliate Scholar, Stanford Center for Internet and Society*
Daniel Kahn Gillmor, Technologist
J. Alex Halderman, Morris Wellman Faculty Development Assistant Professor of Computer Science and Engineering, University of Michigan; Director, University of Michigan Center for Computer Security and Society
Jonathan Mayer, Stanford University*
Patrick R. McDonald, Director of Network Administration and Security, C2FO
Charlie Miller, Security Engineer at Twitter
Peter G. Neumann, Senior Principal Scientist, SRI International, Computer Science Lab, Moderator of the ACM Risks Forum
Ken Pfeil, CISO, Pioneer Investments
Ronald L. Rivest, Professor, MIT
Bruce Schneier, Cryptographer and Security Specialist
Armando Stettner, Internet Technology Consultant
Matt Suiche, Staff Engineer, VMware
Cris Thomas (Space Rogue), Security Strategist at Tenable Network Security*
Dr. Nicholas Weaver, Researcher, ICSI and UC Berkeley

*Titles and affiliations are for information purposes only.