

July 27, 2015

Dear President Obama,

We the undersigned civil society organizations, security experts, and academics write to urge you to strongly oppose the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754).¹ We urge that you pledge to veto CISA, as you did twice during consideration of the similarly flawed Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 3523, H.R. 624).²

The Administration first stated its opposition to CISPA and its intention to veto it because the legislation failed to “preserve[] Americans’ privacy, data confidentiality, and civil liberties and recognize[] the civilian nature of cyberspace.”³ The following year the Administration again voiced strong opposition to CISPA, and set forth the following three overarching priorities that information sharing legislation:

(1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections.⁴

CISA not only fails to adhere to these important principles, it also fails to effectively address the specific concerns that were raised in those previous Statements of Administration Policy.

Concerns Regarding Requirements to Remove Personal Information: Both Statements of Administration Policy on CISPA raised the concern that the bills “lack[ed] sufficient limitations on the sharing of personally identifiable information”⁵ as companies were not required to “take reasonable steps to remove” it.⁶

Similarly, CISA fails to protect users’ personal information. It allows vast amounts of personal data to be shared with the government, even that which is not necessary to identify or respond to a cybersecurity threat. This is because CISA permits companies to leave personal and identifying information in indicators it shares with the government unless the company affirmatively knows that the information is not directly related to a threat⁷ – a condition that would rarely be met. Thus, it allows companies to share virtually all personal and identifying information by default.

¹ Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), <https://www.congress.gov/bill/114th-congress/senate-bill/754>.

² Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011), <https://www.congress.gov/bill/112th-congress/house-bill/3523/titles>; Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013), <https://www.congress.gov/bill/113th-congress/house-bill/624>. See also Exec. Office of the President, Statement of Administration Policy: H.R. 3523 – Cyber Intelligence Sharing and Protection Act, Apr. 25, 2012, https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf [hereinafter “CISPA SAP 2012”]; and Exec. Office of the President, Statement of Administration Policy: H.R. 624 – Cyber Intelligence Sharing and Protection Act, Apr. 16, 2013, https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf [hereinafter “CISPA SAP 2013”].

³ CISPA SAP 2012, *supra* note 2.

⁴ CISPA SAP 2013, *supra* note 2.

⁵ CISPA SAP 2012, *supra* note 2.

⁶ CISPA SAP 2013, *supra* note 2.

⁷ CISA, Sec. 4(d).

Authorization to Use Information in Investigations Unrelated to Cybersecurity: The Administration's opposition to CISA also stemmed from concerns that CISA failed to reasonably limit the authorized uses for the information that companies share with the government. The Administration's position was that "sharing must be consistent with cybersecurity use restrictions, the cybersecurity responsibilities of the agencies involved, as well as privacy and civil liberties protections and transparent oversight."⁸

CISA significantly deviates from these limitations. It 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. CISA would also permit the federal government to use information in investigations in trade secret violations and identity fraud, and under the Espionage Act.⁹ Additionally, CISA authorizes companies to share information with the government for any purpose authorized under the Act, which means that companies could share information for the purpose of investigating these unrelated crimes.¹⁰ While these crimes are serious, there is no justification for undermining the legal protections that currently apply when such investigations are underway, particularly when the data of so many innocent citizens could be affected.

Failure to Establish Civilian Control of Domestic Cybersecurity: The Administration opposed CISA because it failed to follow "the longstanding tradition to treat the Internet and cyberspace as civilian spheres"¹¹ and it "effectively treat[ed] domestic cybersecurity as an intelligence activity."¹² These concerns were rooted in overly expansive use authorizations and in the authorization to share information directly with the National Security Agency (NSA).

CISA also fails to maintain civilian control. In addition to having extremely broad use authorizations, as described above, it 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, including the NSA. While liability protection would only attach for sharing directly to the Department of Homeland Security, this is not an adequate safeguard because the bill permits sharing "notwithstanding any law." Even if information were to be shared with a civilian entity like DHS, CISA would require the government recipient of any cyber threat indicator to automatically disseminate it, without delay or modification to remove personal information, to the Department of Defense and the NSA, and to non-military intelligence agencies.¹³ This undermines both privacy and civilian control.

CISA Raises Additional Areas of Significant Concern: CISA raises many concerns in addition to those outlined above, as its provisions would also be detrimental to Internet security, pose further threats to privacy and civil liberties, and undermine transparency and accountability. First, CISA could undermine Internet security because it authorizes companies to deploy "defensive measures" (also commonly referred to as "countermeasures"), even when the countermeasure would be otherwise illegal under the Computer Fraud and Abuse Act.¹⁴ Second, the definitions for "cyber threat," and "cyber threat indicator," are concerning because they are unnecessarily broad. Finally, the bill would undermine

⁸ CISA SAP 2013, *supra* note 2.

⁹ CISA, Sec. 5(d)(5)(A), and CISA Sec. 4(d)(4)(A).

¹⁰ CISA, Sec.4(c)(1).

¹¹ CISA SAP 2013, *supra* note 2.

¹² CISA SAP 2012, *supra* note 2.

¹³ CISA, Sec. 5(a)(3).

¹⁴ CISA, Sec. 4(b).

transparency by adding the first new exemption to the list of nine other exemptions included in the Freedom of Information Act (5 U.S.C. 522(b)) since it passed in 1966.

CISA fails to address many of the concerns raised about preceding information sharing bills that the Administration opposed, and it threatens to undermine privacy and civil liberties, and increase cyber-surveillance. We strongly oppose CISA and we urge you to again defend privacy and civil liberties by voicing your opposition and your intention to veto it.

Thank you for your consideration.

Sincerely,

Civil Society Organizations and Companies

Access

Advocacy for Principled Action in Government

American Association of Law Libraries

American-Arab Anti-Discrimination Committee

American Civil Liberties Union

American Library Association

Amnesty International

Association of Research Libraries

Benetech

Bill of Rights Defense Committee

Brennan Center for Justice

Council on American-Islamic Relations

Center for Democracy & Technology

Constitutional Alliance

The Constitution Project

Defending Dissent Foundation

Demand Progress

DownsizeDC.org

Electronic Frontier Foundation

Fight for the Future

Freedom of the Press Foundation

Free Press Action Fund

Government Accountability Project

Hackers/Founders

Human Rights Watch

Liberty Coalition

National Association of Criminal Defense Lawyers

New America's Open Technology Institute

Niskanen Center

OpenMedia.org

OpenTheGovernment.org

PEN American Center

Privacy Rights Clearinghouse

Restore the Fourth

RootsAction.org

R Street
Silent Circle
Student Net Alliance
Venture Politics
World Privacy Forum

Security Experts

Jacob Appelbaum, Security and privacy researcher, The Tor Project
Eric Brunner-Williams, Retired
Jon Callas, Cryptographer and Inventor
Antonios A. Chariton, Security Researcher, Institute of Computer Science, Foundation of Research and Technology -- Hellas
John Covici, Systems Administrator, Covici Computer Systems
David L. Dill, Professor of Computer Science, Stanford University
Riley Eller, Inventor and Security Strategist; Chief Technology Officer, CoCo Communications
Rik Farrow, Editor, USENIX
Robert G. Ferrell, Special Agent, Information Security (Ret.), U.S. Dept. of Defense
Bryan Ford, Associate Professor of Computer Science, Swiss Federal Institute of Technology, Lausanne
Dr. Richard Forno, Jr. Affiliate Scholar, Stanford Center for Internet and Society*
Joe Grand, Principal Engineer, Grand Idea Studio, Inc.
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
Carl Hewitt, Board Chair, Standard IoT Foundation
Daniel Kahn Gillmor, Technologist
Ryan Lackey, Computer Security Professional
Christopher Liljenstolpe, Architect, Project Calico, IETF OpenPGP WG Co-chair, past Operations Area Co-Chair, past chief architect for both Cable & Wireless, and Telstra.
Jonathan Mayer, Stanford University*
Steve Manzuik, Director of Research, Duo Security
Andrew McConachie, Internet Infrastructure Engineer
Patrick R. McDonald, Director of Network Administration and Security, C2FO
Charlie Miller, Security Researcher
Prof. Chip Pitts, Lecturer in Law, Stanford/Oxford
Ronald L. Rivest, Professor, MIT
Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School
Space Rogue (C. Thomas), Security Strategist, Tenable Network Security
Armando Stettner, Internet Technology Consultant
Matt Suiche
Dan S. Wallach, Professor, Department of Computer Science, Rice Scholar, Baker Institute of Public Policy, Rice University
Nicholas Weaver, Researcher, International Computer Science Institute
Dr. Stefano Zanero, International Director, Information Systems Security Association

*Titles and affiliations are for information purposes only.