July 15, 2014

President Barack H. Obama
The White House
1600 Pennsylvania Ave
Washington, D.C. 20500

cc: Office of Science & Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Ave
Washington, D.C. 20504

Dear Mr. President,

The undersigned civil society organizations, companies, and security experts are writing to urge you speak out against S. 2588, the Cybersecurity Information Sharing Act ("CISA") of 2014.[1] The bill, which was marked up in a secret, closed session last week, focuses on increasing information sharing between the government and private sector.[2] Having passed out of the Intelligence Committee, the bill is now set to head to the Senate floor with few meaningful privacy protections added.[3]

CISA fails to offer a comprehensive solution to cybersecurity threats. Further, the bill contains inadequate protections for privacy and civil liberties. Accordingly, we request that you promptly pledge to veto CISA. We also request that you issue a similar veto threat for any future legislation that takes a similar approach on information sharing. A robust approach to cybersecurity is necessary to protect the security of the internet and those who use it.

Cybersecurity Legislation

In 2012, the U.S. Congress considered two cybersecurity bills: the Cybersecurity Act in the Senate, and the Cybersecurity Information Sharing and Protection Act ("CISPA") in the House of Representatives.[4] The Cybersecurity Act contained measures directed at consumer education, research, and digital security as well as a narrowly crafted information sharing provision. However, CISPA addressed information sharing alone,

[1] Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014).
[2] "Information sharing" is the term for the process by which private and government entities transfer certain types of data. In cybersecurity legislation, information sharing refers to the information concerning so-called cyber threats, which can include personally identifiable information. Different legislative approaches allow different types of information to be shared. *See, e.g.*, Cybersecurity Information Sharing Act of 2014 § 2(7), 113th Cong. (2014); Cyber Information Sharing and Protection Act § 3(g)(4), H.R. 624, 113th Cong. (2013)
[3] Press Release, Sen. Diane Feinstein, Senate Intelligence Committee Approves Cybersecurity Bill (July 8, 2014) http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=4c0ee3f0-8191-410c-b35d-bfe3bb0b3b46.
[4] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012);.Cyber Information Sharing and Protection Act, H.R. 3523, 112th Cong. (2011).

and the Administration threatened to veto the Bill due to significant privacy concerns and other shortcomings.[5] Both bills failed to pass.[6]

The following year, Executive Order ("EO") 13636 and Presidential Policy Directive ("PPD") 21 were issued.[7] EO 13636 set forth provisions for information sharing while calling for privacy and civil liberties protections to be built into procedures adopted pursuant to it. Despite the issuance of the EO, Congress has continued efforts to pass legislation to further increase the amount of information transferred between the government and the private sector without addressing other important aspects of cybersecurity.

In early 2013, Representative Mike Rogers (R-MI) re-introduced CISPA. CISPA, like CISA, once again only addressed information sharing, and was widely criticized for its failure to limit the amount of personal information the federal government could transmit and store. The Administration threatened to veto CISPA as it moved to the House floor, and the Senate has never considered the bill.

Problems with CISA

CISA presents many of the same problems the Administration previously identified with CISPA in its veto threat.[8] Privacy experts have pointed out how CISA would damage the privacy and civil liberties of users.[9] Language in CISA, like CISPA, also bypasses the Administration's previously stated preference of having a civilian agency lead U.S. cybersecurity efforts in favor of automatic and simultaneous transfer of cybersecurity information to U.S. intelligence agencies, like the National Security Agency.[10]

---

[5] Office of Mgmt. & Budget, Exec. Office of the President, *Statement of Administration Policy: H.R. 624 - Cyber Intelligence Sharing and Protection Act* (2013) http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf ("While there is bipartisan consensus on the need for such legislation, it should adhere to the following priorities: (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.").

[6] CISPA passed the House, but was never considered in the Senate.

[7] Exec. Order No. 13,636, 78 FR 11737 (Feb. 9, 2013); PPD No. 21, (Feb. 12, 2013).

[8] Office of Mgmt. & Budget, Exec. Office of the President, *supra* note 5; Office of Mgmt. & Budget, Exec. Office of the President, *Statement of Administration Policy: H.R. 3523 - Cyber Intelligence Sharing and Protection Act* (2012).

[9] *Letter to Senator Dianne Feinstein, Chairman and Senator Saxby Chambliss, Vice Chairman, U.S. Senate Select Committee on Intelligence* (Jun. 26, 2014) https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/06/CISA-Letter-62614.pdf.

[10] Michelle Richardson, *Keep Domestic Cybersecurity Efforts in Civilian Hands*, American Civil Liberties Union (Apr. 27, 2012) https://www.aclu.org/blog/national-security-technology-and-liberty/keep-domestic-cybersecurity-efforts-civilian-hands.

While amendments attached to CISA during the committee mark-up alleviate concerns about the bill's disproportionate impact on non-U.S. persons, the revised bill fails to correct many of the bill's most basic problems. In fact, while amendments ostensibly require additional limited data use and retention limitations,[11] those provisions are left wide open to secret government interpretation.[12]

Additionally, the Committee failed to respond to many of the serious concerns raised by civil society. For example, the bill still imposes no affirmative duty for entities to strip out personally identifiable information unless the entity has actual knowledge that the identifiable information is present.

CISA authorizes the federal government to use the information in a broad range of investigations and prosecutions, such as Espionage Act investigations, raising questions about increased harm to whistleblowers and journalists.[13] The bill also offers broad immunity protections for corporations, disincentivizing companies from protecting the privacy of users and limiting access to remedy for those whose rights are impacted.[14] Additionally, CISA fails to incorporate any significant lessons learned regarding the critical role of transparency in oversight, providing a broad new categorical exemption from disclosure under the Freedom of Information Act, the first since the Act's passage in 1966.[15]

Because CISA does not remedy any of the failures the Administration previously identified in CISPA and because it fails to adequately protect all users, we request that you promptly pledge to veto this dangerous legislation.

A Comprehensive Approach to Cybersecurity

Cybersecurity legislation that focuses solely on information sharing is inadequate for the modern internet. An emphasis on proper communications security could help

---

[11] Cybersecurity Information Sharing Act of 2014 § 5(b)(2)(B)(ii), (a)(3)(C) 113th Cong. (2014).
[12] *In re. App. Of Federal Bureau of Investigation*, (FISA ct. 2013); Orin Kerr, My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215, The Volokh Conspiracy (Sep. 2013).
[13] *Letter to Senator Dianne Feinstein, Chairman, U.S. Senate Select Committee on Intelligence, et al.*, (Jun. 26, 2014) https://www.aclu.org/sites/default/files/assets/6-26-14_--_cisa_sign-on_letter_final.pdf.
[14] Brandon Moss, *School house lock: How the U.S. government proposes to "protect" your data*, Access Now (Jun. 26, 2014) https://www.accessnow.org/blog/2014/06/26/school-house-lock.
[15] *See* Sandra Fulton, *Beware the Dangers of Congress' Latest Cybersecurity Bill* (June 27, 2014) https://www.aclu.org/blog/national-security-technology-and-liberty/beware-dangers-congress-latest-cybersecurity-bill; *see also* supra note 13.

prevent attacks, rather than reacting to problems as they arise. We believe a far better solution is a comprehensive bill, which should:

1. Create incentives and processes to improve digital security, including resolving known vulnerabilities in a timely fashion,[16] making systems more resilient, and improving security architecture by design;
2. Empower a civilian federal agency to perform the government's information assurance functions. The agency should not have a conflicting mission that would compromise its information assurance tasks;[17]
3. Ensure that all administrative agencies that collect or handle personal information, including the White House, have, on staff, a Chief Information Officer, Chief Privacy Officer, and a Chief Technology Officer with clearly published contact information. These officers should be responsible for establishing and publishing a responsible disclosure policy and process for vulnerability reporting.
4. Provide resources to educate users, companies, and other actors on cybersecurity threats and best practices for avoidance and mitigation;
5. Foster greater international dialogue of communication of cyber conflict red lines; and
6. Establish strong transparency obligations that give as much access as possible to both governmental oversight bodies and the public.

Conversely, an acceptable piece of cybersecurity legislation cannot:

1. Address information sharing alone, which is an inherently incomplete approach to cybersecurity;[18]
2. Inadequately protect individual privacy and civil liberties;
3. Allow the NSA or any military agency to coordinate or play any other central role in civilian cybersecurity policy;[19] or

---

[16] CISA, as it currently stands, does provide a very limited requirement for federal entities to protect their information systems through the use of security controls, but only in certain circumstances in regard to certain databases. Cybersecurity Information Sharing Act of 2014 § 4(d)(1), 113th Cong. (2014). This would not adequately protect sensitive information held by the government. *See, e.g.,* AFP, *Chinese hackers break into US government network* (July 10, 2014) http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10958233/Chinese-hackers-break-into-US-government-network.html.

[17] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Dec. 18, 2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. Any consultation between the information assurance agency and other federal government entities, include the NSA, should be made public and transparent.

[18] We understand that a piecemeal approach may be necessary to ensure that proper parts of cybersecurity legislation are considered by the proper Congressional committees with the proper expertise. However, if that is the case then we would highlight the need to focus more on communications security provisions, many of which are non-controversial, and which should be either considered and passed first, or in close conjunction to information sharing provisions.

4. Inappropriately conflate cyber crime or other online activities with cyber war or acts of cyber warfare.

Guidance for robust cybersecurity legislation can be found in the *Guidelines for the Security of Information Systems*, published in 1992 by the Organisation for Economic Co-operation and Development ("OECD").[20] The Guidelines focused on a holistic approach to cybersecurity, enumerating nine principles to "foster confidence in information systems." The experts who contributed to the OECD process recommended a comprehensive approach to cybersecurity that included, among other things, allocation of risks and liabilities, education and training for developers and law enforcement, and recourse and redress for violations of rights. The Guidelines should be used as a resource for lawmakers in crafting a cybersecurity bill.

Conclusion

The current discourse centered solely on information sharing mistakenly focuses on only one layer of the internet to the detriment of all actors in the online ecosystem. A comprehensive approach to cybersecurity, as laid out here, would both defend and extend civil liberties and the right to privacy of users globally.

Legislation that focuses exclusively on facilitation of information sharing, such as CISPA and CISA, jeopardizes the foundation of cybersecurity by improperly pitting human rights against security. We urge you to pledge to veto CISA and all future legislation that takes a similar approach.

---

[19] *See* Electronic Privacy Info. Center, *Comments of the Electronic Privacy Information Center to the National Institute of Standards and Technology, U.S. Department of Commerce* (Apr. 8 2013) http://epic.org/privacy/cybersecurity/EPIC-Comments-NIST-Cybersecurity-Framework.pdf ("The overwhelming majority of cybersecurity incidents do not fall within the "national security" designation. As Deputy Secretary Lute has noted, cyberspace should not be managed like a warzone. Most of the cybersecurity issues amount to civilian crimes committed in cyberspace (i.e. cybercrimes) that should be handled by state and local law enforcement and not under the rubric of national security."); *see also* American Civil Liberties Union, *More About Department Of Defense/NSA Spying* (Jan. 22, 2013) https://www.aclu.org/spy-files/more-about-department-defensensa-spying ("This ideal was finally codified after the Civil War through the Posse Comitatus Act, which prohibited the Army from engaging in law enforcement activities on U.S. soil..").

[20] Org. for Econ. Co-operation and Dev., *OECD Guidelines For The Security of Information Systems And Networks: Towards a Culture of Security* (Aug. 6, 2002) *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm.

July 15, 2014

Please direct your response to Amie Stepanovich at Access [amie@accessnow.org, 888.414.0100, x702] and she will share it with the other signatories.

Sincerely,

Access
Advocacy for Principled Action in Government
American Civil Liberties Union
American Library Association
Amicus
Center for Democracy and Technology
Competitive Enterprise Institute
CREDO
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DuckDuckGo
Electronic Frontier Foundation
Fight for the Future
Freedom of the Press Foundation
Free Press Action Fund
The Libertarian Party
Liberty Coalition
Media Alliance
New America Foundation's Open Technology Institute
OpenMedia.org
OpenTheGovernment.org
Participatory Politics Foundation
PEN American Center
Reddit
RootsAction.org
Silent Circle
Student Net Alliance
The Sunlight Foundation
TechFreedom

Jacob Appelbaum
Matt Blaze
Matthew D. Green
Morgan Marquis-Boire
Eleanor Saitta