April 20, 2015

Dear Representative:

We, the undersigned civil society organizations, security experts, and academics write to urge opposition to the Protecting Cyber Networks Act (PCNA, H.R. 1560)[1] if it comes to the House floor for a vote. PCNA seriously threatens privacy and civil liberties, and would undermine cybersecurity, rather than enhance it.

Like its Senate counterpart, the Cybersecurity Information Sharing Act (CISA, S. 754)[2], PCNA 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 surveillance activities.

PCNA 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 urge you to oppose PCNA 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:** This could result in the unnecessary scrutiny of innocent Internet users online activities, and sharing of their personal information, and information about that Internet use, including content of their online communications.[4]

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

---

[1] Protecting Cyber Networks Act (PCNA, H.R. 1560), https://www.congress.gov/bill/114th-congress/house-bill/1560.

[2] Many of the undersigned groups have signed letters strongly opposing CISA for many of the same reasons detailed in this letter. *See* Coalition Letter Opposing CISA as Reported Out of Committee (April 20, 2015) (on file with New America's Open Technology Institute); *and* Coalition Letter Opposing CISA Discussion Draft (March 2, 2015), https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/03/CISA-2015-Sign-On-Letter.pdf.

[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; the absence of a sunset; and 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.

[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.

information.

- **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 crimes and activities that have nothing to do with cybersecurity, such as robbery, arson, carjacking, or any threat of serious bodily injury or death, regardless of whether the harm is imminent. The use authorizations included in this bill undermine traditional due process protections, and turn PCNA into a cyber-surveillance bill rather than a cybersecurity bill[5]; and

- **Authorize companies to deploy invasive countermeasures, euphemistically called "defensive measures":** The authorization for deploying defensive measures is narrower than in other bills, however PCNA still authorizes an entity to deploy a defensive measure that gains unauthorized access to computer systems of innocent third parties who did not perpetrate the threat, an action that would otherwise violate the Computer Fraud and Abuse Act. It may also authorize defensive measures that unintentionally harm innocent third parties. [6]

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

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

---

[5] 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.
[6] Notably, PCNA limits countermeasures to those "operated on and the effects of which are limited to" one's own system, or another information system upon written consent of its owner (Sec. 3(b)(1)). In contrast, CISA requires countermeasures be "applied to" one's own network, but does not limit off-network effects that harm third parties. The narrower authorization in the PCNA is undermined by an ambiguous limitation to which the authorization is subject. The limitation suggests that a company may deploy a defensive measure that *unintentionally* destroys, disables, or substantially harms an information system owned or operated by a third party that has not consented to the operation of such countermeasures.

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
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

Security 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, 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
C. Thomas (Space Rogue), Security Strategist, Tenable Network Security*
Dr. Nicholas Weaver, Researcher, ICSI and UC Berkeley