April 21, 2015

Dear Member:

The undersigned open government and civil liberties groups write in opposition to H.R. 1560, the Protecting Cyber Networks Act ("PCNA"). Although less pernicious than its Senate counterpart, the Cybersecurity Information Sharing Act ("CISA"), the PCNA would undermine government transparency and potentially result in the bulk collection and mining of sensitive personal information by intelligence agencies that would have little to do with cybersecurity.

The bill set for floor consideration this week would increase access by intelligence agencies like the NSA to sensitive personal information without adequate legal protections against the use of "cyber threat" information to investigate whistleblowers or against activities similar to the secret mass surveillance programs revealed over the past two years.

It would also categorically exempt information provided to the government from disclosure under the Freedom of Information Act ("FOIA") and create a new secret cyber-intelligence coordinating body under the Director of National Intelligence ("DNI"). Both the FOIA exemption and the new DNI entity threaten to increase government secrecy and consequently heighten the potential for abuse.

With respect to the possibility this could become a "cyber-surveillance" bill, section 4(d)(5) of the PCNA would permit the federal government to use so-called "cyber threat indicators" received from the private sector, which may include sensitive personally identifiable information unrelated to the cyber threat, for a wide variety of law enforcement purposes, including "preventing, investigating, disrupting, or prosecuting" violations of the Espionage Act and a wide variety of other federal crimes.

The authorization to use cyber threat information in Espionage Act cases is particularly worrisome in light of the increasing use of that law as justification for the surveillance of journalists and their sources, and the criminal prosecution of those sources. The Obama administration has pursued more "leak" prosecutions than all other presidencies combined. This provision, when combined with other vague or overbroad definitions in the bill, could be used to justify searches of journalists' communications with sources and whistleblowers' communications with Congress.

Unlike CISA, the PCNA would not create an entirely new exemption from FOIA, the first since the mid-1980s. This is a welcome omission. Unfortunately, however, the PCNA would exempt from disclosure, "without discretion," information provided to the government under section 552(b)(3)(B) of FOIA and under all state sunshine laws. This discretion-less withholding is unnecessary given that the bill already clarifies that information provided to the government will have been shared "voluntarily." That creates a legal presumption against disclosure under the

existing exemption four in FOIA for confidential commercial information. At the very least, the PCNA should delete the term "without discretion."

Additionally, the PCNA would create an entirely new coordinating body at the DNI, the Cyber Threat Intelligence Integration Center ("CTIIC"). Civilian cybersecurity is a civilian mission, and it must be housed in a civilian agency to ensure appropriate transparency safeguards and accountability. We are concerned that the CTIIC, which would have broad authority to receive information shared under the PCNA and share it across the intelligence community, will add an unnecessary layer of additional secrecy here, which would shield abuse from public and congressional scrutiny.

We do acknowledge the efforts of members of the House intelligence committee to include better privacy protections than CISA, which would be an unmitigated disaster for accountability and civil liberties. Unfortunately the protections in this law do not go far enough, and it will, if passed, both increase government secrecy and potentially result in surveillance abuses.

We look forward to working with Congress to ensure that any cybersecurity legislation passed into law protects both our nation's computer networks and our civil liberties, while preserving and promoting transparency and accountability to the public. If you would like to discuss these issues further, please contact Patrice McDermott, Executive Director of OpenTheGovernment.org, at 202-332-6736 or pmcdermott@openthegovernment.org, or Gabe Rottman, legislative counsel with the American Civil Liberties Union, at 202-675-2325 or grottman@aclu.org .

Sincerely,

Access
Advocacy for Principled Action in Government
American Association of Law Libraries
American Civil Liberties Union
American Library Association
American Society of News Editors
American-Arab Anti-Discrimination Committee
Association of Alternative Newsmedia
Association of Research Libraries
Campaign for Liberty
Center for Effective Government
Center for Media and Democracy
Constitutional Alliance
Council on American-Islamic Relations
CREW
Cyber Privacy Project
Defending Dissent Foundation
Electronic Frontier Foundation
Essential Information

Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project
Hackers/Founders
National Coalition Against Censorship
No More Guantanamos
OpenTheGovernment.org
PEN American Center
Progressive Librarians Guild
Project Censored
Project On Government Oversight
Public Record Media
Society of Professional Journalists
Sunlight Foundation
Venture Politics