The Honorable John Boehner
Speaker of the House
United States House of Representatives
H-232, U.S. Capitol
Washington, DC 20515

The Honorable Nancy Pelosi
Democratic Leader
United States House of Representatives
H-204, U.S. Capitol
Washington, DC 20515

Dear Speaker Boehner, Democratic Leader Pelosi, and Members of the House of Representatives:

As advocates of constitutionally limited government and free markets, we write to express our concerns about the National Cybersecurity Protection Advancement Act (NCPAA) of 2015. Specifically, we urge lawmakers to:

1. Include a 3-year sunset,
2. Preserve common law remedies,
3. Bar regulatory coercion of information-sharing,
4. Improve reporting requirements regarding how often private data are shared under the bill as cyber threat indicators (CTIs),
5. Enhance agency accountability,
6. Suppress evidence unlawfully obtained as CTIs from use in criminal cases,
7. More thoroughly bar use of CTIs for regulatory purposes, and
8. Clarify language authorizing defensive measures.

The Federal government can and should do more to deter attacks on private networks and systems, help the victims of such attacks identify the culprits, and educate companies about impending cyber threats from terrorist organizations and foreign governments. This will, in turn, protect the privacy of users who rely on those companies to safeguard sensitive data like email and Internet usage history. The NCPAA does much to facilitate sharing by government of CTIs with private companies, which will help private companies defend their networks, infrastructure and themselves.

We share the concern of private companies that existing privacy statutes unduly impede their ability to lawfully share information with one another and with government agencies — if only by creating legal uncertainty that could cause delay in urgent decisions about what kind of information to share when a company is under attack or perceives indications about a coming

attack. For instance, the Wiretap Act[1] and Stored Communications Act[2] allow companies to monitor their networks and share CTIs to protect their own systems but not to protect third-party systems.

This is emblematic of a larger problem in attempting to legislate or regulate around the Internet: government rarely gets it exactly right — and, worse, is generally slow to correct its mistakes. For these reasons, we believe that *any* complex law governing the Internet should require periodic reauthorization to help ensure that it does not distort the market, especially in ways that harm user privacy. We urge you to add a 3-year sunset — or, at a minimum, the same 5-year sunset contained in the Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in 2012 (H.R. 3523) and in H.R. 624 (2013).

> **Amendment #1 (3-Year Sunset)**: Replace "*Sec. 14. SUNSET.*" with the following text: "*This Act, and the amendments made by this Act, shall cease to have effect on the date that is 3 years after the date of enactment of this Act*."

The stakes here are high: the bill defines the key term "cyber threat indicator" so broadly that it includes private information. As a result, NCPAA would create a sweeping immunity for companies to share private information with each other — and with the government. Unlike immunity provisions in previous cybersecurity information sharing bills, this immunity would not void private contracts or terms of service. It is critical that companies be allowed to make enforceable promises to their users governing how they share potentially sensitive information. Otherwise, the market will not be able to function: companies will be unable to compete on privacy and will have no incentive to offer greater levels of privacy protection or enter into enforceable codes of conduct governing information-sharing. We urge you to resist any attempt to water down this provision (Section 3(i)(11)(D)(i) of H.R. 1731).

However, while the bill rightly preserves the sanctity of contract and implicitly allows for Federal Trade Commission enforcement of terms of service and codes of conduct, the bill fails to maintain other common law actions. We urge you to ensure that the bill's immunity focuses only on *statutory* restrictions that might discourage information-sharing.

> **Amendment #2 (Protect Common law Remedies):** Add a new subparagraph to section 3(i)(11), at page 44, line 23: "*(J) COMMON LAW.—Nothing in this section may be construed to limit the liability of any non-Federal entity to any person for any claim at, or arising out of, common law.*"

Like previous cybersecurity bills, the bill is ostensibly intended to facilitate voluntary sharing of CTIs. The bill generally bars coercion of such sharing but is overly narrow in its list of tools the government may not use to "encourage" sharing. Thus, it would likely not stop the Federal

1. *See* 18 U.S.C. § 2511(2)–(3).
2. *See* 18 U.S.C. § 2702(b).

Communications Commission from using its free-wheeling merger review process to extract nominally voluntary concessions that it could not legally require from telecom companies regarding information sharing — something the agency does routinely in other contexts. Proposed legislation would give the FTC similarly broad discretion in deciding whether to certify multistakeholder codes of conduct regarding privacy and data security, which could allow the FTC to extract concessions regarding information-sharing with government, such as watering down procedures for removing personal information from CTI.

> **Amendment #3 (Coercion of Info Sharing)**. Section 3(i)(11)(E)(iii), at page 43, lines 17–20, bars any Federal entity from "condition[ing] the award of any Federal grant, contract, or purchase on the sharing of cyber threat indicators or defensive measures with a Federal entity." Add, after "purchase" in line 18, the phrase "*license, certification, or any benefit*."

Of course, no one really knows how much personal information might be shared under the bill as CTI — and, no matter what the legislation does to ensure that information sharing is voluntary, we may never know what kind of power government might exert over private companies. To that end, it is critical that, as Congress considers reauthorizing NCPAA in the future (ideally, five years after passage), lawmakers have a clear sense of just how much private information is actually being shared under the bill.

If, contrary to our expectations, private companies systemically err on the side of sharing personal information unrelated to cyber threats with government agencies, the balance struck in this bill between privacy and security might not be the right one — and we might support, for example, imposing greater duties on private companies to remove unnecessary private data from information they share. Accurate and comprehensive data will be critical in measuring the bill's true consequences. Unfortunately, we have seen in other areas that government agencies have little incentive to report data that could reflect unfavorably on their programs. And here, the issue is difficult, because we do not want to force government to dig more deeply into CTI data than necessary, lest reporting requirements actually increase privacy invasions.

> **Amendment #4 (Enhance Reporting Requirements)**: Sections 3(i)(7)(B)(i)(II), at page 32, and 3(i)(7)(C)(i)(II), at page 34, require Federal and State/local/tribal governmental entities, respectively prior to sharing CTI, to remove PII that "is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident." Amend Section 3(i)(6)(D), at page 28, to require statistics on how often such data is removed and what kind of data it is. This will tell us how much private data private companies are sharing with the government that government believes, at the time, is unnecessary to pass on to other agencies or private companies.

We fear that the bill does not do enough to ensure that government agencies actually follow NCPAA's requirements in handling personal information that might be contained in CTIs shared with government. The bill should ensure that those harmed by a government employee's

disregard for NCPAA's requirements have legal recourse even if they cannot prove the violation was intentional.

> **Amendment #5 (Ensure Agency Accountability)**: In Section 3(i)(9)(A), at page 38, lines 13–14, change "intentionally or willfully" to "*intentionally, willfully, or recklessly*."

Similarly, the bill fails to stop government entities from using CTIs for law enforcement purposes unrelated to cybersecurity. The bill should include the same suppression of unlawfully obtained evidence found in 18 U.S.C. § 2515 — instead of merely offering criminal defendants civil damages (and a prison sentence). Unlike Section 2515, however, the bill should not limit the ability of private entities to use cyber threat indicators in civil litigation — though such entities should face potential liability for breach of contract or under the private right of action.

> **Amendment #6 (Add Suppression Remedy)**. Add a new paragraph between Sections 3(i)(9) and 3(i)(10) at page 40, line 3: "*(10) PROHIBITION OF USE AS EVIDENCE OF UNLAWFULLY OBTAINED CYBER THREAT INDICATORS.—Except as authorized by paragraphs (6) and (7) of this subsection, no part of any cyber threat indicator obtained or disclosed by a Federal entity or other governmental entity under this Act, and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof*."
>
> **Conforming amendment**: Add a new clause at the beginning of Section 3(i)(9)(D), at page 40, line 3, so it reads "*Except as provided in paragraph (10), a cause of action under this subsection* …" (leave the rest of the subparagraph intact).[3]

By the same token, government should not be able to use CTIs for "regulatory purposes," something the bill attempts to prevent. But the ambiguity of that term might allow regulators to claim that this term pertains only to rulemakings, and not to other forms of regulation.

> **Amendment #7 (Bar Use of CTIs for Any Regulatory Purpose)**: Section 3(i)(7)(B)(ii)(II), at page 33, lines 11–13, provides that CTIs "may not be used by the Federal Government for regulatory purposes." Add *"whether through rulemaking, enforcement actions, license issuance or transfer, merger review, or other means."*

3. Here, paragraph (10) refers to the new paragraph added in the previous amendment, assuming the original paragraph (10) is renumbered (11).

Conforming amendment: Section 3(i)(7)(C)(ii)(II), at page 36, line 2, add the same text: "*"whether through rulemaking, enforcement actions, or other means."*

Finally, Section 3(i)(5) authorizes "defensive measures" unless it "destroys, renders unusable, or substantially harms an information system or data on an information system." This broad definition could encourage counter-attacks upon innocent third parties and the perusal and even copying of private information found on their systems. The key technical problem is that many cyber attacks are conducted through "botnets" composed of the systems of innocent third-parties without their knowledge. In such a scenario, it may be impossible for the victim to distinguish between the true perpetrator and other victims. The simplest way to deter harmful over-reaction would be to clarify that the bill does not immunize against violations of the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030).

Amendment #8 (Clarify Defensive Measures Language). Add a new subparagraph to section 3(i)(11), at page 44, line 23: "*(K) COMPUTER FRAUD AND ABUSE.—Nothing in this section may be construed to limit the criminal or civil liability of any non-Federal entity for accessing any computer without authorization in violation of section 1030 of title 18, United States Code.*"

We urge you to consider these amendments as you mark up the bill in order to ensure that the bill does not unintentionally harm the very consumers it is ultimately intended to protect.

Respectfully,

TechFreedom

Competitive Enterprise Institute

Center for Financial Privacy and Human Rights

FreedomWorks

Institute for Policy Innovation

Liberty Coalition

Niskanen Center