April 21, 2012

The Honorable Mike Rogers
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives
Washington, D.C. 20515

The Honorable C.A. Dutch Ruppersberger
Ranking Member
Permanent Select Committee on Intelligence
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Rogers and Ranking Member Ruppersberger:

As public interest groups dedicated to free enterprise and limited government, we applaud bipartisan congressional efforts to streamline laws governing the sharing of "cyber threat information." Empowering the private sector to defend itself against cyber adversaries is an important and constitutional governmental function. By removing legal obstacles to cyber threat information sharing among private and governmental entities, Congress can ensure that companies are equipped to safeguard their systems and users against attacks that threaten the nation's welfare and security.

However, the Cyber Intelligence Sharing and Protection Act of 2011 ("CISPA"), even as modified by the April 19 bill version, risks unduly expanding federal power, undermining freedom of contract, and harming U.S. competitiveness in the technology sector. To remedy these serious concerns, we urge CISPA's sponsors to amend the bill to address the following recommendations.

CISPA Should Respect Freedom Of Contract And Privacy Competition

While CISPA enables companies to restrict how cyber threat information they share may be used by other entities, the bill's sweeping immunity provision effectively denies providers the ability to make enforceable promises to impose such restrictions on third parties. Thus, under CISPA, a provider could not meaningfully assure users it will not share their information with government unless compelled to do so by valid legal process. Nullifying such voluntary agreements undermines the ability of companies to compete on privacy protection, and risks chilling the adoption of cloud technologies by businesses and individuals concerned about their sensitive data (*e.g.*, trade secrets, private e-mails) winding up in the wrong hands. Therefore, CISPA should explicitly state that it does not supersede private contracts that limit further disclosure and use of cyber threat information.

CISPA Should Limit Governmental Use Of Shared Information To Cyber Threats

CISPA wisely bars the federal government from using cyber threat information "for regulatory purposes." But the bill permits all other governmental uses so long as "at least one significant purpose" of such use is for "cybersecurity" or the "protection of [U.S.] national security." Thus, if a federal agency received a private e-mail pertaining to not only a cyber threat but also, for instance, to a criminal violation of the Internal Revenue Code or the Archaeological Resources Protection Act,[1] that agency could share the e-mail with any other governmental entity for use in criminal prosecution. Permitting government to access citizens' information for the purpose of investigating and prosecuting non-cybersecurity offenses, without a warrant based upon probable cause to believe such non-cybersecurity offenses have been committed, violates the Fourth Amendment right to be secure against unreasonable searches and seizures. CISPA should proscribe all governmental use and sharing of cyber threat information for purposes unrelated to cybersecurity, except when reasonably necessary to avert immediate danger of death or serious bodily harm.

[1] *Cf.* Brian Walsh, *Wall Street Journal Exposes Federal Overcriminalization*, Heritage Foundation Foundry Blog, July 28, 2011, http://blog.heritage.org/2011/07/29/wall-street-journal-exposes-federal-overcriminalization/.

CISPA Should Deter Reckless Information Handling By Government

CISPA creates a limited private right of action allowing individuals whose information has been improperly used or shared by a governmental entity to recover actual damages. But for an aggrieved party to prevail, it must show the governmental entity "intentionally or willfully" violated the statute. Imposing such a high burden on potential plaintiffs will under-deter governmental agencies from negligently handling private information. Therefore, CISPA's private right should also allow individuals to recover damages for grossly negligent violations by governmental entities.

CISPA Should Only Immunize Reasonable Cyber Threat Information Sharing

CISPA immunizes covered private firms that share "cyber threat information" for a "cybersecurity purpose" with any other entity—private or governmental—from *all forms* of civil and criminal liability. This sweeping provision would go so far as to immunize a provider that shares information *unrelated* to a cyber threat, so long as that provider believes in "good faith" that its actions accord with CISPA—even if the provider fails to take reasonable steps to verify prior to sharing information that it actually pertains to a cyber threat. CISPA should only immunize companies for sharing information when they have an objectively reasonable belief that it pertains to a cyber threat.

CISPA Should Bar Government From Coercing Firms To Share Information

Although CISPA's "anti-tasking" restriction bars the government from conditioning a private entity's access to cyber threat information on that entity's own willingness to share, the bill ignores an even greater threat of tasking: the federal government's ability to leverage grants or procurement contracts to pressure companies to disclose cyber threat information. CISPA should contain an enforceable ban on such *quid pro quos* to deter potential abuse by federal agencies, some of which have historically leveraged the procurement process to strong-arm private entities into facilitating mass digital surveillance.[2]

CISPA's Definition Of 'Cyber Threat Information' Should Be Narrowed

CISPA's definition of "cyber threat information" encompasses, among other things, "information directly pertaining to" threats involving efforts to "degrade" networks, "misappropriat[e]" "private information," or gain "unauthorized access" to a system. This broad definition is not necessarily limited to information that actually describes or identifies specific cyber attack threats. Especially problematic is the term "unauthorized access," which in related contexts has been broadly construed to include violations of a website's terms of service.[3] While we recognize the pitfalls of defining "cyber threat information" too restrictively, CISPA's definitions should be narrowed to focus on genuine cyber threats.

CISPA Should Provide For Meaningful Independent Oversight

CISPA calls for the Inspector General of the intelligence community to submit annual reports to Congress on the use of cyber threat information. But to ensure truly effective oversight, the independent Privacy and Civil Liberties Oversight Board—which has been inactive for years—should also be involved. CISPA should require Congress to appoint a roster of independent experts to the PCLOB, reallocate the trivial amount of funding needed for Board's operations from elsewhere in the federal budget, and ensure that the Director of National Intelligence consults the Board in crafting CISPA procedures.

Conclusion

We applaud the Committee's well-intentioned efforts to enhance our nation's cyber defenses. If CISPA is not revised to reflect our concerns, however, it may have serious unintended consequences for America's vibrant technology sector—and for our constitutional rights. Therefore, we urge CISPA's sponsors to consider these recommendations before sending the bill to the House floor.

---

[2] For instance, former Qwest CEO Joseph Nacchio alleged in a 2007 court filing that when Qwest refused to participate in an NSA surveillance program, the agency "retaliated by not awarding lucrative contracts to Qwest." Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, Wash. Post, Oct. 13, 2007, at A1, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485_pf.html.

[3] *See* Orin Kerr, *Ninth Circuit Hands Down En Banc Decision in United States v. Nosal, Adopting Narrow Interpretation of Computer Fraud and Abuse Act*, The Volokh Conspiracy, April 10, 2012, http://volokh.com/2012/04/10/ninth-circuit-hands-down-en-banc-decision-in-united-states-v-nosal-adopting-narrow-interpretation-of-computer-fraud-and-abuse-act/.

Respectfully,

Ryan C. Radia
Associate Director of Technology Studies
Competitive Enterprise Institute

Berin Szoka
President
TechFreedom

Wayne T. Brough, Ph.D.
Chief Economist and Vice President of Research
FreedomWorks

William Wilson
President
Americans for Limited Government

Michael D. Ostrolenk
Co-Founder/National Director
Liberty Coalition

Al Cardenas
Chairman
American Conservative Union