CRITICAL PROBLEMS WITH CISPA

The Cyber Intelligence Sharing and Protection Act (CISPA, or H.R. 624) has eight critical problems that threaten civil liberties and render the bill unacceptable.

Critical Problem #1: The bill undermines civilian control of the government's cybersecurity program because it permits companies in the private sector to share cyber threat information derived from users' communications directly with the National Security Agency, a secretive military intelligence agency. The information shared can include communications content. The sharing is authorized even if it would otherwise be prohibited by a privacy law. A company that shares this information in good faith is completely immunized against any liability.

> **Solution:** Permit companies to share narrowly defined cyber threat information with the Department of Homeland Security's National Cybersecurity and Communications Integration Center. *[See insert to p. 4]*

Critical Problem #2: The bill risks turning cybersecurity into a backdoor wiretap by permitting cyber threat information shared with the government to be used for non-cyber national security purposes, and because its law enforcement use restrictions apply only to the Federal government.

> **Solution:** Strike the authorization to use for national security purposes cyber threat information shared under the bill. Extend law enforcement use limits now applicable only to the Federal government to state, local and tribal governments. The bill would still permit governmental entities to use cyber threat information for cybersecurity purposes, to prosecute cybersecurity crimes, to protect against imminent danger of serious bodily harm, and to protect children against child pornography, risk of sexual exploitation and serious threats to their physical safety. *[See amendments to p. 10, p. 11 strike of lines 1-2, and p. 18 strike of lines 1-7]*

Critical Problem #3: The cyber threat information that can be shared is too broadly defined. Information that merely "pertains" directly to four categories cyber threats and vulnerabilities can be shared notwithstanding any law, and there is no requirement to strip out personally identifiable information unrelated to the threat.

> **Solution:** Require that cyber threat information be "reasonably necessary" to describe the threat or vulnerability, and that reasonable efforts to strip out irrelevant personally identifiable information be undertaken before the cyber threat information is shared. *[See pp. 19-20]*

Critical Problem #4: The bill authorizes and immunizes the use of "cybersecurity systems" to identify and obtain cyber threat information without limiting the scope of such use to the network or information of the entity being protected. This could authorize reaching into the networks of others -- hacking that would otherwise be a crime under the Computer Fraud and Abuse Act (CFAA).

> **Solution:** Instead of using overbroad terms and pre-empting the CFAA and all other laws, simply permit companies to monitor for cyber threat information their own networks and the networks of companies that have hired them to provide cybersecurity services. *[See insert to p. 4]*

Critical Problem #5: The bill gives companies that act in good faith complete immunity for any "decisions made based on cyber threat information identified, obtained or shared" under the bill. This is too open-ended. For example, a company's decision to hack into a user's computer to obtain information it believes was taken from it without its authorization, and in doing so, to render the user's computer inoperable, would be completely immunized against liability to the user even though it is a cybersecurity crime under the bill.

> **Solution:** Grant companies that act in good faith immunity for monitoring and information sharing activities permitted under the bill, but not for all "decisions made" based on cyber threat information received or obtained. *[See p. 9 strike of lines 6-9]*

Critical Problem #6: The bill does not require companies that receive cyber threat information to use it only for cybersecurity purposes.

> **Solution:** Require companies that use CISPA authorities to receive shared threat information, or monitor to obtain threat information, to use it only for cybersecurity purposes. *[See p. 6 lines 19 and 21]*

Critical Problem # 7: The authorization to share information pre-empts all law rather than specifying the laws to which an exception is being made. This endangers civil liberties and is almost certain to have unintended results.

> **Solution:** Specify the laws being pre-empted, including the electronic surveillance law and anti-trust laws as appopriate. *[See insert to p. 4]*

Critical Problem #8: The bill lacks adequate oversight provisions. Importantly, it does not empower the Department of Homeland Security to set information sharing rules, privacy safeguards and minimization procedures that will protect privacy and civil liberties. It also fails to require reports by the Privacy and Civil Liberties Oversight Board and by the privacy and civil liberties officers of key agencies.

- **Solution:** Require DHS, with DOJ approval, to issue policies and procedures governing use, retention, disclosure and destruction of cyber threat information to protect privacy and civil liberties, and require PCLOB and privacy and civil liberties officer reports consistent with those found in S. 3414 (112th Congress, the "Lieberman bill") Sections 704(g)(3)-(5). (END)