Association for Computing Machinery (ACM)
US Public Policy Council of ACM (USACM)

1828 L Street NW, Suite 800
Washington, DC 20036
Main Phone: 212-626-0541
acmpo@acm.org

ACM US Public Policy Council

June 6, 2012

We are writing with comments on the Cyber Intelligence Sharing and Protection Act (CISPA). We are the US Public Policy Council of ACM (USACM), a community of technical experts representing ACM — the Association for Computing Machinery — a major technical and professional society involved in all aspects of computing and information technology, including cybersecurity.

USACM appreciates that enhanced sharing information regarding threats and incidents may have potential benefits for cybersecurity, but we have serious concerns regarding the framework established by CISPA. We have analyzed the current version of CISPA against our general recommendations on cybersecurity legislation (please see attached) and have found a number of significant issues in the bill with respect to privacy.

The benefits of increased information sharing should not -- and need not -- come at the expense of substantially increased privacy risk.[1] USACM's privacy recommendations (also attached), the internationally recognized Fair Information Practice Principles, and the federal Privacy Act of 1974 *all* stress that the collection of personally identifiable information (PII) should be minimized so as to include only that which is necessary for a stated purpose. Additionally, the use and retention of PII should be limited to that stated purpose. CISPA exhibits particular weaknesses in these areas of data minimization and retention.

CISPA does not provide any guidance, nor does it propose any mechanism for producing guidance, about the circumstances under which PII may be reasonably determined to be cyber threat information and thus appropriately shared with the federal government. It is left to covered entities to decide what PII to share with the government, with the only restrictions being those they choose to place upon themselves. Combined with the expansive definition of "cyber threat information" —which could encompass everything from port scans to destruction of entire networks—the absence of any relevance test or standard provides no meaningful support for collection minimization. Not only is this contrary to good privacy practices, it may also result in a torrent of insignificant information, possibly overwhelming the Government's analytical capability.

Similarly broad are the expressed purposes for which the information, including any PII, may be used by the government. In particular, the provision (Section 1104 (c)(1)(E)) for using such information to protect the national security of the United States would permit many possible

[1] The 2010 U.S. National Security Strategy views safeguarding privacy and civil liberties as integral to protecting our nation's digital infrastructure: "Our digital infrastructure, therefore, is a strategic national asset, and protecting it — while safeguarding privacy and civil liberties — is a national security priority." (http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, p. 27)

uses having nothing to do with cybersecurity. Thus, the actual permitted uses of shared information, including PII, go beyond the purported reason for collecting the information.

While CISPA does prohibit the government from using particular types of PII—e.g., educational and medical records (Section 1104 (c)(4)), these restrictions are narrow and fail to address the wide variety of possible PII that may be available. While there is a requirement to inform entities when shared information is determined not to be cyber threat information, there is no accompanying requirement that the government destroy such information. This amplifies the impact of absent standards regarding sharing of PII.

We note the mandate in CISPA to "make reasonable efforts to limit the impact on privacy and civil liberties of the sharing of cyber threat information," but other provisions of the legislation run counter to that mandate. Moreover, this provision, like others, fails to invoke any framework, standards, oversight, or controls to be used toward this end or any mechanism for establishing them. Such a vague standard will make responsible implementation difficult. More effective measures to minimize the collection, sharing, and retention of cyber threat information will also provide a security benefit by reducing the amount of information that could be targeted by data thieves and that would need to be stored and analyzed by the government. Having meaningful oversight and boundaries will help to ensure that information is properly used without creating new risks.

More effective information sharing in support of cybersecurity is a laudable goal, but CISPA is seriously flawed in its approach to PII. Better approaches to information sharing are certainly possible if privacy goals are also considered. If we can provide additional information or assist in any other way with this process, please contact our Public Policy Office at 212-626-0541.

Sincerely,

Eugene H. Spafford, Ph.D.
Chair
U.S. Public Policy Council
Association for Computing Machinery