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

April 8, 2013

The Honorable Mike Rogers
Chairman, House Intelligence Committee
2121 Rayburn House Office Building
Washington, D.C. 20515

The Honorable C.A. 'Dutch' Ruppersberger
Ranking Member, House Intelligence Committee
2416 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Rogers and Ranking Member Ruppersberger:

We are writing to express our concerns with the Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 624. We are the U.S. 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. We commented on the prior instance of the bill in June 2012, and have attached a copy of those comments to this letter.

Given that this year's version of the legislation is nearly identical to the version from 2012, our concerns expressed in our comments last year remain. While we agree with the goal of the bill – a more secure cyberspace — as we wrote last year[1], "[t]he benefits of increased information sharing should not -- and need not -- come at the expense of substantially increased privacy risk." Not only might individuals suffer serious harm, but loss of privacy represents a serious security risk in and of itself. Individuals whose information has been exposed may be induced to make the system vulnerable, through social engineering attacks (e.g., clicking links in plausibly personalized emails), embarrassment, blackmail, or intimidation.

The legislation would be improved by providing more explicit guidance on minimizing the risk of disclosure of personally identifiable information (PII) or other sensitive business and/or personal information. For instance, if the legislation were to encourage specific practices – such as data de-identification – to mitigate disclosure risks, then relevant standards could be referenced (e.g., the Federal Trade Commission standard for de-identification outlined on page 20 of its 2012 Privacy Report[2]). We also recommend there be an explicit time limit placed on PII shared under this legislation, such that information must be deleted after a set time period rather than held indefinitely. Further, in keeping with established privacy principles, information shared under this statute should not be usable for any purposes not related to the purpose for which it was shared – cybersecurity.

The potential for abuse and theft of information must be better balanced with the need to share threat information. As currently written, the proposed legislation could allow sharing of *any*

[1] http://usacm.acm.org/images/documents/USACMCISPAStatement.pdf

[2] http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

information about any persons without particular cause, effective oversight, or meaningful recourse. At a minimum, the bill should contain explicit limits on what may be shared absent a warrant, and include specific oversight mechanisms. In the spirit of well-established privacy principles, the legislation should explicitly establish the following with respect to any information shared under this act:

- Shared data is to be used only for cybersecurity purposes specified in this act
- Shared data is to be kept for at most a limited time (e.g., 6 months) and deleted by all receiving parties thereafter
- Each receiving party must institute a process for periodic review of data received, and deleting data no longer necessary to support the purposes of this act
- When erroneous data is discovered, it should be deleted immediately, and any parties sharing that erroneous data must be notified of the errors within a short time (e.g., 10 days)
- All data shared under this act will include indications of its origin, the dates when it was shared with each party, and the date on which it will be deleted
- All data shared under this act will be de-identified whenever possible
- Use of received data for any criminal prosecution requires a supporting subpoena or warrant
- All data shared under this act will be protected against unauthorized or accidental disclosure, modification, or other access

As computer scientists, we understand the complexity and difficulties involved in trying to balance the many interests involved in sharing cybersecurity threat information. Should you have questions about our concerns, or about other related topics, we would be happy to discuss them with you further. Please feel free to contact our Public Policy Office at 212-626-0542 or at acmpo@hq.acm.org

Regards,

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