usacm ACM US Public Policy Council

The Honorable Lamar Smith
Chair, House Judiciary Committee
2409 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Conyers, Jr.
Ranking Member, House Judiciary Committee
2426 Rayburn House Office Building
Washington, D.C. 20515

January 17, 2012

Dear Chairman Smith, Ranking Member Conyers, and members of the Judiciary Committee:

We welcome your recent announcement that the DNS blocking provisions will be removed from the Stop Online Piracy Act (SOPA — H.R. 3261) until further study is conducted. The attached document was written before that announcement, but we believe that it may assist you as your committee gives further consideration to intervention in DNS operation. Our analysis of the bill with those provisions has revealed significant technical concerns with some of these items.

As introduction, the US Public Policy Council of ACM (USACM) is 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. Many members of ACM rely on intellectual property rights to protect their writings, software products, and inventions. Our Code of Ethics and Professional Conduct requires members to honor intellectual property rights including copyright and patents. Thus, we support efforts to address criminal violations of intellectual property laws.

Our understanding of the bill's provisions to disrupt advertising and payment processing of rogue sites is that they seem to be reasonable and may have some positive effects. However, the forced removal of sites from indexing and search sites is more problematic, particularly because it is trivial and quick (a matter of minutes) to register new domain names, then inject them into the indexing sites. As such, the rogue sites will be back in the indices far faster than new court orders may be obtained to exclude them. Thus, this provision is likely to have little effect other than to burden the courts and companies that provide important services to the public, such as search sites.

Moreover, our analysis of the portions of this legislation that dealt with DNS (Domain Name System) revealed them to be misguided. They would undermine years of sound technical work by the international community — and substantial progress made by the federal government toward addressing troubling security flaws in our existing DNS system. We note that those security problems — the very problems that the DNS Security Extensions (DNSSEC) are intended to address — were labeled (in aggregate) one of the two biggest threats to the Internet by the National Academies in the 1999 study *Trust in Cyberspace*,[1] and in the 2003 White House report *National Strategy to Secure Cyberspace*.[2] Any actions that interfere with or weaken any aspect of DNSSEC should thus be viewed with grave concern.

The Committee received numerous comments about SOPA and how it would affect DNS. Further, the Committee received considerable information about how DNS works. As a result, the Committee attempted to address technical concerns within the manager's amendment by adding "safe harbor" provisions to the legislation. **While we appreciate the Committee's attempt toward addressing the technical concerns, the proposed legislation — even with the manager's amendment — would still impose significant negative consequences on the proper functioning of the Domain Name System, and especially with the ongoing implementation of DNSSEC. The approaches in the bill would ultimately prove ineffective in addressing the legislation's goals (and they are already easily bypassed), and will impose cost burdens on innocent third parties.**[3]

We cannot ignore the fundamental facts that govern the core technical operations of the Internet and the importance of moving toward DNSSEC, both to provide better security and to help prevent forms of fraud and other crimes. Interfering with DNS resolution is thus in opposition to initiatives by the Department of Defense, the Department of Homeland Security, U.S. law enforcement, and Internet security experts: The proposals affecting DNS in the SOPA legislation would require significant interference with DNSSEC — operators cannot reliably block offending sites with DNSSEC and so would have been faced with the choice of abandoning DNSSEC or being in violation of issued court orders.

Furthermore, SOPA included a fundamental shift away from consensus-based international standards for ensuring that the Internet functions in a flexible, robust, seamless, efficient and secure way to an approach of unilateral action by a government into how critical technical aspects of the Internet are to function. This change is in opposition to efforts being conducted by (at least) the Departments of State and Commerce. SOPA also would have set a dangerous precedent that could have had unfortunate future effects.

We recommend that the best course of action for any such legislation is to avoid technology mandates. Computing technology evolves quickly, and innovations often

[1] http://www.nap.edu/openbook.php?record_id=6161

[2] http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[3] We note that many of these concerns also exist with the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act, or PIPA) in the Senate.

render old technologies moot. Mandated technological approaches that are likely to be rendered obsolete in short order may nonetheless chill or prevent research and innovation within the US, while having little impact on U.S. competitors and domestic firms outside the U.S. These approaches may also have the negative side-effect of encouraging firms to move offshore and beyond the reach of our laws. This particular legislation also could impose undue costs on U.S. ISPs, search firms, and other entities. Such results would seem untoward given the current economy and the vital roles being played by information technology firms.

Attached is our in-depth discussion of DNS, DNSSEC, and analysis of SOPA (as well as PIPA insofar the provisions around DNS filtering overlap). The document expands on several of the items we mention above, and provide more detail on the interference with the DNSSEC.

Thank you for considering our views. Should you have any questions please feel free to contact us at 202 659-9712.

Signed

Eugene H. Spafford, Ph.D.
USACM Chair

cc: House Judiciary Committee Members

ABOUT ACM AND USACM

ACM, the Association for Computing Machinery is the world's oldest and largest educational and scientific computing society, uniting over 110,000 computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities.