July 29, 2011

To whom it may concern:

Thank you for accepting comments on the "Cybersecurity, Innovation and the Internet Economy" green paper. On behalf of StopBadware, a nonprofit, anti-malware organization based in Cambridge, Massachusetts, I submit the following comments.

One question raised in the Green Paper is how to incorporate consumer and civil society views into discussion about cybersecurity. Because few consumers are likely to engage directly with Department of Commerce efforts in this space, I encourage the Department to work closely with organizations that represent the needs of, and engage directly with, consumers. Typically, these will be public charity nonprofit organizations. In addition to organizations focused specifically on security, such as StopBadware and the National Cyber Security Alliance, several consumer protection organizations, such as Consumers Union and Consumer Action, are likely to take an interest. These organizations are well positioned to be informed about the complexities of security technology and policy. They also have experience communicating complex ideas clearly to broad public audiences.

Another area of inquiry in the Green Paper is how to identify security best practices applicable to the I3S environment and how to create incentives for the practices' adoption. StopBadware has found that the web hosting industry lacks clear guidance about how hosting providers can combat badware, and that natural market conditions are at times insufficient to get providers to do so. To address the first issue, StopBadware developed—in consultation with a cross-industry working group—the first installment in what will become a collection of best practices documents for web hosting providers. The first document, which focuses on how providers should respond to reports of badware on their networks, can be found on our website[1]. To create an incentive for adoption of the best practices, StopBadware will soon offer a free seal that hosting providers can display if they pledge to institutionalize the practices in their environments. Such seals have proven effective at driving baseline privacy and security practices in other contexts.

Positive recognition of compliance is not always sufficient to drive business behavior. One approach that StopBadware has used with modest success is "naming and shaming." StopBadware has historically published "top 50" lists of networks and IP addresses by number of badware URLs. These lists often receive attention from web hosting providers that wish to ensure they do not remain near the tops of these lists, and therefore take aggressive action to remove badware from their networks.

Where even reputation fails to drive positive behavior, liability must be considered. Safe harbor provisions that provide immunity from liability for providers that engage in "appropriate" behavior to combat badware

[1] http://www.stopbadware.org/best-practices/web-hosting-providers

may be a viable option. This would, however, require both a more fully developed code of conduct for providers and a legal framework that establishes both liability and the safe harbor. StopBadware commissioned a legal white paper[2] by the Cyberlaw Clinic at Harvard University's Berkman Center for Internet & Society. It describes the current state of case law on this topic in the U.S. and concludes that web hosting providers, in general, are *not* liable for addressing badware, even where they are aware of badware hosted on their systems. It should be noted that changing the law to assign liability to providers would run into substantive concerns about the appropriate role of intermediaries and the challenges of providers conclusively distinguishing badware from other content.

Closely related to the need for web hosting providers to address badware effectively is the need to improve the reporting of badware by those who discover it (e.g., security professionals) to those best equipped to address it (e.g., hosting providers, domain registrars, and owners of compromised websites). While there have been several recent efforts to develop standards for the exchange of technical data related to badware[3], there has been less focus on what information should be reported to whom, and when. To help address this, StopBadware has assembled a cross-industry working group to develop best practices for badware URL reporting. This document is expected to be released later this summer. There is also a need to invest in the automation and centralization of such reporting. The former will increase the efficiency of reporting (and, hopefully, remediation), while the latter will provide aggregated data to help identify the providers most and least responsive to abuse reports.

The Green Paper also solicits comments on the role of the Department in promoting public-private partnerships to improve I3S security. StopBadware encourages the Department to identify areas in which educational resources and market-based mechanisms can be combined to address large scale problems. One such problem is encouraging and supporting consumers and small businesses in removing badware from infected computers and other devices. A closely related, but operationally distinct, issue is supporting a similar constituency in remediating compromised websites that facilitate the spread of badware. In both cases, the I3S can and should be integral to identifying the infected devices and sites, notifying affected parties, and providing tools to assist with remediation. There is a need, however, to coordinate this work to create a streamlined user experience, eliminate duplication of effort, and develop valuable aggregated data.

In Germany, an independent organization—supported initially by government—plays this coordination role. It ensures a cohesive flow of information from security organizations to ISPs to affected users. It also provides the victims with educational content and tools to help them remove badware and protect their devices from future infection. The Department of Commerce should consider playing a similar role in establishing such a system in the United States, perhaps with an addition of a market-driven mechanism for connecting users with value-added products and services to supplement the free offerings from the independent organization.

StopBadware and a coalition of supporting companies are driving a similar approach for compromised websites. Private parties, such as Google and Mozilla, detect badware websites and warn users to avoid them. These notifications prompt the owners of compromised sites to seek remediation assistance. StopBadware provides a free, centralized set of resources to provide such assistance. These resources include objective educational content, a volunteer-driven online community, and a process for requesting that warnings be removed for websites that were wrongly identified or that have been cleaned. The Department may wish to

---

[2] Attached.

[3] See, for example, IODEF, MAEC, the IEEE ICSG malware reporting format, and MARF.

study this multi-stakeholder initiative to identify lessons that can be applied to efforts in other areas. In addition, as the I3S is both a critical component of—and a major beneficiary of—this work, the Department might consider opportunities to contribute to its growth and success.

StopBadware welcomes the opportunity to further engage with the Department of Commerce on the ideas above and on other ways in which the public, private, and nonprofit sectors can work together to combat badware and other security threats.

Sincerely,
Maxim Weinstein
Executive Director