BEFORE THE

DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

DEPARTMENT OF HOMELAND SECURITY

IN THE MATTER OF "MODELS TO ADVANCE VOLUNTARY CORPORATE NOTIFICATION TO CONSUMERS REGARDING THE ILLICIT USE OF COMPUTER EQUIPMENT BY BOTNETS AND RELATED MALWARE."

DOCKET NO. 110829543-1541-01

COMMENTS OF THE
UNITED STATES INTERNET SERVICE PROVIDER ASSOCIATION

The United States Internet Service Provider Association ("US ISPA") hereby offers its comments in response to the Request for Information ("RFI") from October 4, 2011 concerning approaches to creating a voluntary industry code of conduct to address the detection, notification and mitigation of botnets.

OVERVIEW

Founded in 2002, US ISPA is an association of businesses that operate Internet networks and/or provide Internet services. Its members include Internet Service Providers (ISPs), network operators and providers of Internet portals and other online services. US ISPA participates on behalf of these industries in conferences, panels and government proceedings.

US ISPA was founded to focus on a discrete set of policy and legal concerns common to the Internet service provider industry, primarily law enforcement compliance and security matters, including cybersecurity. US ISPA's members are very active in a number of public-private partnerships focusing on both physical and cyber security; the companies develop and implement preparedness strategies for crisis events, participate in the development of industry standards and sound practices, manage 24x7 operational and technical centers, and regularly engage in pertinent policy issues. As an organization, US ISPA examines these issues with its industry partners on the Communications Sector Coordinating Council and through the federal legislative process.

Sound security practices are core to the business of ISPs. Every day providers are vigilant against a wide variety of threats. Employing robust, nimble and effective security is essential when operating networks and offering Internet-based communications services.

Providers offer myriad security solutions to customers of all sizes - enterprise, small business and consumers. All ISPs oversee the security of their networks and have internal

procedures to deal with a wide range of of threats. Some ISPs offer services and software today to identify malware, notify the customer and even aid in remediation. Those services are offered as competitive products, and it is not unreasonable to expect that more companies will be promoting new services for the consumer in the future.

ISPs do play a useful role in cybersecurity, and there are specific functions that ISPs are best suited to provide. In some cases, the ISP may be the best positioned to take action, but there is nothing preventing others to act. Focusing on the role of the ISP and potential coercive measures the ISP could apply, exemplified in the codes of conduct from other nations, is misguided, particularly since it is not yet clear that the approaches adopted elsewhere—heavily focused as they are on ISP notification via email or other means to end users—are cost-effective or efficient. Examples from other countries are not necessarily applicable to the American marketplace where competition is robust and there is a competitive environment for anti-malware and security products in general. The United States is unique in its impressive scale of Internet users and the variety of platforms through which customers communicate, and such a shallow international comparison trivializes the differences in cultural, legal and technical structures.

By issuing an RFI in this space, there is a presumption that intervention by the government is needed to help spur attention and activity, but as stated above, the ISP community is very active in targeting and addressing a wide range of security threats. There is nothing to support a compelling need for specific government action.

I. ANY EFFORT TO REDUCE MALWARE MUST BE INCLUSIVE OF THE ENTIRE INTERNET ECOSYSTEM.

It is positive to convene a discussion on the security threats facing the Internet industry and the roles and responsibilities across government and the private sector; however any discussions must include participation from entities in all varieties of services. This would include sectors like software developers, anti-virus vendors, firewall manufacturers, and providers of Internet-based content, applications and services, as well as ISPs. The RFI particularly targets the Internet service provider community suggesting that ISPs, "[have] contact information for the end-user and a pre-existing relationship." Software vendors, anti-virus companies, application service providers and financial service companies have verified contact information and a pre-existing relationship with their customer as well, yet these parties are not subject to scrutiny in the government's action item.

ISPs recognize the role they can play in providing security capabilities to end users and for some, it may be one of notification and detection; however the community of experts is broader and more varied than a single segment of the Internet industry. Success will depend on the involvement of companies beyond the Internet service provider community.

II. THERE IS NO ONE-SIZE-FITS-ALL SOLUTION TO COMBATING CYBER THREATS.

Because the threat environment changes rapidly, there is no simple turn-key solution available today to eradicate botnets and fight malware. Success in combating cyber threats depends on technical proficiency, innovation and flexibility, not prescribed solutions focused on the action of a small number of stakeholders. The government should champion a layered defense; a resilient, multi-faceted approach to fighting malware, not a finite structure that weighs heavily on one segment of industry.

ISPs and other Internet participants must be free to innovate and implement a variety of tools across their networks and services, and to offer them in a competitive environment. Such a complex security challenge requires a range of ever-evolving security solutions.

III. VOLUNTARY INITIATIVES MUST BE DEVELOPED AND LED BY THE PRIVATE-SECTOR.

Any initiative that is labeled as "voluntary" must be developed and led by the private sector. The voluntariness of an approach laid out by the government in an RFI is illusory.

Industry must be able to develop new products and capabilities with the certainty that any partnerships with the government are directed toward fighting security threats, not toward mitigating the threat of regulation. Government is best positioned to support the private-sector by serving the function of law enforcement and in a more positive way, like assisting with education and awareness, as opposed to offering and mandating solutions in a form of regulation. Even if a method is presented as voluntary, if it is suggested by and

promoted by the government, it can become the de facto solution. In that same vein, government-driven solutions tend to obtain input from companies able to dedicate resources to work with and influence the government. Smaller players, who may not have the resources to participate in such activities, may not have their voices reflected in any such centralized outcomes. The government should not want to prejudice the outcome by influencing the activities undertaken by the private-sector.

There are industry groups that have been specifically studying how best to mitigate botnets and malware for some time. The Messaging Anti-Abuse Working Group, or MAAWG, is composed of technical representatives from across the private-sector and has been actively working on the issue. A group like MAAWG may well be better positioned to implement something like the RFI envisions, making it truly a voluntary, industry-led effort.

Leadership from the government may be useful in some areas; but any specific direction from governmental entities would be problematic.

IV. THE ROLE OF THE GOVERNMENT IS IMPORTANT, ALBEIT LIMITED IN SCOPE.

While it is imperative for the government to take the lead in certain aspects of cybersecurity, the role of the government is limited in scope. While not an exclusive list, we suggest three areas where the government could properly lead: 1) education and awareness, 2) to provide a clear legal framework, and 3) to investigate crimes and prosecute criminals.

The government is uniquely situated in being able to reach every household in America, and can play a crucial role in consumer education and awareness. Internet safety and security is a concern of many different departments and agencies across the federal government, and there is a strong desire to ensure U.S. households have the tools they need to keep their computers safe. Organizations the government supports could be leveraged to continue developing coordinated campaigns promoting Internet safety practices. Also, if the parties agree, we believe there could be value in creating a resource center for end users seeking additional computer health tools.

There remains legal uncertainty in the area of cybersecurity. There is a real need to examine the current legal regime and assess where changes could be made to support the respective roles and responsibilities of the government and the private sector. This must be conducted with an eye to balancing the needs of security with the privacy rights of U.S. customers. The government can lead by working with industry and lawmakers to develop a clear legal framework for a modern, competitive Internet age.

Even as ISPs' networks are rich with cybersecurity solutions, the laws have not evolved to address the diversity and sophistication of the cyber capabilities. Uncertainty and confusion in the law directly result in slow adoption of private-sector security solutions. The government should move to update the law, where appropriate. Eliminating barriers, particularly in the area of information sharing, while ensuring that privacy issues are appropriately addressed, would work toward improving Internet security.

Only the government can investigate and enforce the laws by prosecuting criminals. The ISP industry strongly supports providing law enforcement with the proper resources and tools to investigate and bring to justice cyber criminals.

Finally, the government must lead by example and speak with one voice on cybersecurity matters. Botnets are but one aspect of an overall approach to improving cybersecurity. Multiple, at times conflicting or duplicative, efforts are underway across various government agencies, and all demand attention from the private-sector. Conflicting or duplicative efforts are wasteful and counterproductive – industry resources are stretched trying to give the proper attention to all.

CONCLUSION

The ISP industry recognizes it has an important role to play in helping to fight Internet security threats. We take this role seriously and will continue to develop and offer diverse and dynamic security solutions to our customers. We encourage other participants in the Internet ecosystem to work with us and our partners in the public sector in making available the most robust security defenses available to protect end users from malware. The government does have a critical role to play, and those activities should be supported and undertaken with haste. At this time, however, there is no need for the government to

intervene in the form of leading or directing voluntary development of a code of conduct focused on ISPs.

Respectfully submitted,

UNITED STATES INTERNET SERVICE PROVIDER ASSOCIATION

Kate Dean
U.S. Internet Service Provider Association
700 12th St., N.W.
Suite 700E
Washington DC 20005
+1.202.904.2351

November 14, 2011