Before the
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

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 NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

William Check, Ph.D.
Senior Vice President
Science & Technology
And Chief Technology Officer

Rick Chessen
Neal M. Goldberg
Loretta P. Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W., Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

November 14, 2011

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

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 NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association (NCTA) hereby submits its comments in response to the Request for Information (RFI)[1] issued by the Department of Commerce and the Department of Homeland Security in the above-captioned proceeding.[2]

INTRODUCTION AND SUMMARY

NCTA commends the Departments of Commerce and Homeland Security for their leadership in enhancing the Federal government's awareness of, and response to, the rapid proliferation of botnets and the risks they create for networks, businesses, government, and consumers. Botnets represent a serious cybersecurity issue that implicates national security and economic policy concerns. Network operators are already responding to this threat with a wide array of deterrence and remediation measures. In concert with network providers and other

[1] Department of Commerce, National Institute of Standards and Technology, National Telecommunications and Information Administration; Department of Homeland Security, *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, 76 Fed. Reg. 58466 (Sept. 21, 2011) ("RFI").

[2] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $170 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 23 million customers.

Internet ecosystem participants, there is also an important role for the Federal government in helping to develop a thoughtful and pragmatic policy in this area that helps foster cooperative efforts among industry participants while avoiding mandates.

As the nation's largest provider of high-speed Internet, NCTA's members have strong incentives to ensure the safety and security of their networks. These built-in incentives have spurred several NCTA members to develop bot notification programs that alert subscribers whose devices have been infected and offer solutions and resources for removing malware from their computers. NCTA's members also are at the forefront of developing innovative programs for their customers aimed at deterring infections and notifying affected customers when attacks occur. They also take proactive measures to enable customers to remediate, where possible, disruptions and damage caused by malware, viruses, bots, and other cyber threats that affect the safety and security of both the network and customer devices connected to that network.

While the problems presented by botnets are relatively new, the dangers they pose are real and the breadth and sophistication of botnet threats continues to expand. Botnet attacks can threaten all elements of the broadband ecosytem – the physical network layer, operating systems, applications, and end-user points – and such threats are sophisticated, hard to trace, and generally executed using a combination of resources that are located both within and outside of U.S. borders. Successful efforts to prevent or limit the effect of botnet attacks therefore require cooperation among all participants in the Internet ecosystem, such as operating system vendors, security companies, and application vendors, as well as the efforts of individual Internet Service Providers ("ISPs").

In addition to their individual efforts, cable operators have been active participants in several inter-industry groups combating botnets and other cyber threats, including the Messaging

Anti-Abuse Working Group ("MAAWG") and the Federal Communications Commission's ("FCC's") Communications Security, Reliability and Interoperability Council ("CSRIC"). In connection with their anti-botnet initiatives, NCTA encourages the Departments of Commerce and Homeland Security ("the Departments") to leverage the resources and organizational infrastructure of these inter-industry groups and public-private partnerships. NCTA agrees that voluntary and reciprocal partnerships among all segments of the broadband ecosystem and the government can enhance these efforts. The instant RFI offers a useful vehicle for establishing this partnership.

More generally, the Federal government has an important role to play by ensuring that ecosystem participants can share threat information freely and by providing – between government and industry, and among industry entities – for the discussion and development of detection and remediation techniques. Timely and full information sharing among all affected entities is a cornerstone of effective anti-botnet policy, and the government can help foster that objective by addressing the potential legal issues that could hamper real-time, comprehensive sharing of all relevant information.

The government should also take steps to promote international coordination among ISPs and other stakeholders, since the botnet threat is global in scope. The global scale and pervasive interconnectedness of today's highly complex digital information and communications infrastructure constitutes both a strength and a vulnerability, offering would-be malefactors an almost infinite number of entry points through which to launch clandestine botnet attacks and electronic larceny schemes against networks, businesses, and individual end users.

The growing sophistication of botnet threats underscores the importance of ensuring that network providers and other affected entities have considerable flexibility to address and respond

to those threats. Indeed, imposing a single standard or approach, rather than permitting numerous and varied responses, could have the effect of enhancing the risk from botnets by enabling bad actors to attack multiple networks simultaneously if they are able to circumvent that approach. The developers of the software that create botnets are responsive to any countermeasures by the security industry and have the capability to rapidly engineer responses to a defined set of countermeasures.

It is therefore vital that network providers and other affected entities have the flexibility to respond to real-time botnet threats in a manner that minimizes delay, and maximizes initiative and innovation. Flexibility is also necessary in light of the variations in technology, business models, service, and application vendors, and customer devices employed by each network operator, which may require different tools and practices for detecting and addressing botnet problems. Detection and remediation approaches that might work for some providers may not be viable or optimal for others. Government-prescribed rules and protocols for responding to and remediating botnet threats would be disastrous. There is clearly no "one size fits all" model for either unleashing – or addressing and remediating – botnet threats.

I. CABLE COMPANIES ARE ACTIVELY ENGAGED IN BOTH CONSUMER-FACING AND INTER-INDUSTRY EFFORTS TO ADDRESS BOTNET THREATS

A. Cable Companies Have Responded to Market-Based Incentives to Ensure Online Security for Subscribers by Developing Innovative Offerings to Combat Botnet Attacks

As the nation's largest providers of high-speed Internet service, serving over 45 million customers, the cable industry has a strong and unwavering interest in ensuring a safe and secure network environment for its subscribers. NCTA's members recognize that trust is a key ingredient in building and maintaining a successful relationship with their high-speed Internet customers. Preventing, detecting, and solving botnet threats faced by our customers is not only

an important policy concern, it is also a key business and customer relations issue for NCTA's members – and for other ISPs as well.

End-users are an integral part of the Internet's "network of networks" and can serve as the launching pad for distributed targeted attacks on the entire infrastructure. Botnets are particularly insidious because they turn ordinary users into unwitting participants in the criminal enterprises facilitated by botnets by allowing malefactors to take control of a user's device and use it for their own nefarious purposes. Thus, a bot can cause significant harm to both the individual user and to the entire network and beyond. Because botnets are typically composed of common consumer devices, a consumer-focused approach to cybersecurity is essential to protect both the individual consumers and the broader infrastructure.

Cable operators recognize that consumer-based security tools need to work in conjunction with network-based measures to help secure networks and safeguard end users from botnet threats. NCTA's members have therefore invested substantial resources to deploy state-of-the-art technologies and applications in their networks to combat bots and other forms of malicious and harmful Internet activities. At the customer level, cable operators have instituted comprehensive security offerings to foster a safe and secure network environment for their customers. These programs provide free tools and software to enable cable customers to protect their computers from cyber-attacks and loss or corruption of data.

Comcast's Constant Guard Protection Suite is one example of the type of comprehensive security systems currently offered by cable ISPs to protect end-users' privacy, identity, and digital assets. Constant Guard offers a multilayered, holistic approach to Internet security that provides prevention, detection, and recovery support at both the network and user device levels. Constant Guard combines extensive technological resources, including software such as the

Norton Security Suite, anti-phishing and anti-spyware technology, secure data backup and sharing, identity protection, DNS security, social networking, and online reputation protection tools with an extensive educational program, customer support, and strategic partnerships with related industry experts. It also provides brand new protections designed to address the growing bot problem by integrating anti-keystroke logging technology with a secure log-in. Unlike traditional anti-virus approaches that focus solely on protecting the computer or device, Constant Guard protects the user's personal information and privacy by concealing typed characters, safeguarding credit card information, protecting and remembering passwords, and providing one-click secure login to bank, shopping, and any other online accounts. The Constant Guard Protection Suite is offered to all of Comcast's Xfinity High-Speed Internet subscribers at no additional cost.

Cox, Charter, Time Warner Cable, and Insight Communications also provide comprehensive security suites to their high-speed internet subscribers at no additional cost. Cox subscribers can download the Cox Security Suite Plus Powered by McAfee, which provides anti-virus, anti-spam, anti-spyware, anti-phishing, and email and instant message protection features, as well as SiteAdvisor Plus website rating on up to five PCs or Macs.[3] Cox customers also can install a security package that includes McAfee's Family Protection, which lets parents block access to certain websites, social networks and other online threats.[4]

Charter provides its subscribers with security awareness and education materials, free online scanning and virus removal tools, links to third-party resources (*i.e.*, OnGuard Online,

---

[3] About Cox Security Suite Powered by McAfee, http://ww2.cox.com/residential/centralflorida/support/internet/article.cox?articleId={0b7d0470-6409-11df-ccef-000000000000} (last visited October 26, 2011).

[4] Todd Spangler, *Cox Proffers Free Security Software, Backup for Broadband Subs*, Multichannel News (October 4, 2011), http://www.multichannel.com/article/474785-Cox_Proffers_Free_Security_Software_Backup_For_Broadband_Subs.php.

INOBTR.org, Common Sense, Point Smart Click Safe), and security alerts. Charter also offers a comprehensive "Charter Security Suite," featuring automatic updates that protect against all types of malicious software, automatic virus removal, spyware detection and removal, firewalls with application control, and advanced "in the cloud" technology to provide protection against unknown or unidentified threats.[5]

Time Warner Cable and Insight Communications offer their customers security suites that include anti-virus, anti-phishing, and anti-spam software, a personal firewall, and parental controls at no extra cost to the subscriber.[6] Many cable operators provide updates on the latest threats, ways for customers to report security violations on their systems, such as spam, hackers and other threats, and advice on how to remove offending malware.

Cable operators also are providing automatic bot notification to all subscribers, regardless of whether they choose to download the operators' security offering. For example, irrespective of whether a subscriber obtains Constant Guard, Comcast identifies infected computers using data from reputable Internet research groups that specialize in bot identification, including a list of Internet Protocol (IP) addresses that are infected and those that belong to bot command and control channels. Comcast then looks for malicious behavior exhibited by bots such as spam, distributed denial of service attacks, and repeated connections requests to known command and control channels. This information is aggregated to confirm whether one or more of a user's computers has been infected. Comcast then notifies the user via email or browser notification

---

[5] Charter Security Suite Overview, http://www.myaccount.charter.com/customers/supportgeneral.aspx?pagetype=1 (last visited Nov. 9, 2011).

[6] Internet Security, http://www.timewarnercable.com/nynj/learn/hso/security.html (last visited Oct. 26, 2011); Security, http://www.myinsight.com/Product-Broadband-Security.asp (last visited Oct. 26, 2011).

and directs the user to the Constant Guard Center where he or she can find the resources needed to safely remove the malicious bot.[7]

Time Warner Cable, Insight Communications, and others also provide proactive bot notification for all of their High-Speed Internet subscribers. These programs provide alerts and notices to Internet access customers whose devices have been infected and offer suggestions and resources for remediating the problem. Insight Security Notices direct infected users to the Insight Security Center, where they can access the resources needed to remove the bot safely. In cases where users are not able to disinfect their machines on their own, Insight's Senior Technical Support Technicians are available for consultation on specialized computer services. Time Warner Cable's notifications include information on the exact malware infection and give advice and clear guidance to customers, directing them to trusted tools that will remove the specific malware infecting their machine.

Cox employs a graduated response system, beginning with email notifications. If the infection cannot be removed or if the device comes under repeated attack, Cox consumer support will make direct telephone calls to the subscriber to investigate and provide technical service as needed. BendBroadband employs Cisco System's Ironport appliance to capture and isolate email botnets. BendBroadband also monitors data usage and analyzes usages patterns for signs of botnet infection. Infected hosts are quarantined in order to prevent the spread of infection to others in the network until such time as BendBroadband customer support is able to make contact with the subscriber to resolve the issue. While BendBroadband subscribers may opt out of this service if they choose, only a handful (less than 0.1%) of subscribers have elected to do so.

[7] Comcast affords the customer two options: (1) a do-it-yourself option with step-by-step, self-guided instructions by constant guard; and (2) a signature support option with round-the-clock access to U.S.-based technical experts on bot and virus removal.

Importantly, none of these notification programs result in the termination of subscribers. Subscribers are nearly all innocent victims of botnet attacks and the focus of all these programs is on helping the customer get their devices disinfected, either through specific instructions and tools, or by directing them to a landing page where they can obtain information on additional resources and measures to solve their problem. While there are limited circumstances in which Internet access for some customers may be temporarily suspended pending remediation of the problem, *e.g.*, where devices are compromised by a gated walled garden or subject to an infection that threatens network security, this occurs infrequently and full Internet access is restored once the affected customers have taken the necessary steps to disinfect their devices.

B. The Cable Industry Is Actively Engaged in Inter-Industry Initiatives and Public-Private Efforts to Combat Botnet Threats

In addition to these individual activities, cable operators recognize that detecting and combating botnet threats requires a cooperative effort among ISPs and other stakeholders. To this end, cable operators play an active role in joint public-private efforts and inter-industry initiatives aimed at addressing critical cybersecurity issues, including botnet threats. The FCC's Communications, Security, Reliability, and Interoperability Council (CSRIC), for instance, has served as an important forum for developing best practices and voluntary mechanisms to meet cyber security threats, while promoting the use of innovative and flexible tools to respond to real-time cyber incidents. Comcast, Time Warner Cable, and Cox executives served on the CSRIC II full committee, while Jennifer Hightower of Cox Communications and Michael O'Reirdan, Comcast's Distinguished Engineer, both serve on the recently chartered CSRIC III

full committee.[8] Mr. O'Reirdan is also the chair of CSRIC III's Working Group 7, which focuses specifically on the issue of botnet remediation.[9]

As noted in the RFI, in December 2010, CSRIC's Working Group 8 ("WG8") developed 24 Best Practices to address protection against botnets. WG8 members spent twelve months investigating and addressing issues in the area ISP Network Protection, with a particular focus on the serious and growing problem of bots and botnets. WG8 examined existing best practices and, in consultation with industry experts and other stakeholders, identified 24 Best Practices for prevention, detection, notification, mitigation, and consumer privacy considerations.

The cable industry has also been active in a number of other Federal and non-Federal initiatives that are addressing cyber security policies and practices, including the National Security and Telecommunications Advisory Committee ("NSTAC"), the National Communications Center ("NCC") and the Communications Sector Coordinating Council ("CSCC").[10] NSTAC, for example, has recommended combating botnets through increased international cooperation and partnerships and the development of international cyber-incident warning and response capabilities.[11]

---

[8] *See* FCC, *Communications Security, Reliability & Interoperability Council (CSRIC) Members, at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/List%20of%20CSRIC%20Members.pdf (last visited Nov. 9, 2011).

[9] CSRIC III Working Group Descriptions and Leadership *available at* http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions.pdf (last visited Nov. 9, 2011).

[10] CSCC coordinates, among other things, industry-led initiatives to improve the physical and cyber security of communications sector assets, facilitate the flow of relevant information within the sector and to designated Federal agencies, and to address issues related to response and recovery to large-scale cyberattacks. In 2010, CSCC completed a plan addressing specific cybersecurity policies and practices for communications networks. U.S. Dep't of Homeland Security, *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* at 2 (2010), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf.

[11] NSTAC, "Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability", May 21, 2009, available at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf.

Cable industry engineers in network operations and management also participate in the Messaging Anti-Abuse Working Group ("MAAWG") and the Quality and Reliability Committee of the Institute for Electrical and Electronics Engineers ("IEEE"), and the Internet Engineering Task Force ("IETF") – each of which is engaged in initiatives related to botnet threats as part of their broader cybersecurity activities. IETF, for example, has just recently drafted a memorandum addressing bot remediation issues for ISPs.[12] MAAWG has been particularly active in developing voluntary practices that could serve as a framework for botnet remediation, and has published several reports and comments on the issue, drawing from technical experts, researchers, and policy specialists from a broad base of ISPs and Network Operators representing over one billion mailboxes and from key technology providers, academia and volume sender organizations.[13] Comcast's Michael O'Reirdan currently serves as Chairman of the MAAWG, and Time Warner Cable's Chris Roosenraad is the Vice-Chairman. Comcast, Cox, Time Warner Cable, Charter and Cablevision are each full or sponsor level members of the working group. In addition, there are several cable-specific working groups and activities in this area led by the Society of Cable Telecommunications Engineers ("SCTE") and Cable Television Laboratories, Inc.

MAAWG has submitted its own comments in this proceeding, and NCTA encourages the Departments to consider its recommendations. Notably, MAAWG has recognized that cable operators and other ISPs are not the only entities with interests in and responsibilities for

---

[12] *Recommendations for the Remediation of Bots in ISP Networks*, authored by Jason Livingood, Nirmal Mody, and Mike O'Reirdan, published Oct. 26, 2011. *Available at* http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-18.

[13] *See, e.g.* Nirmal Mody, Michael O'Reirdan, Sam Masiello, and Jason Zebek, *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*, Messaging Anti-Abuse Working Group (July 2009) ("*Best Practices Report*"), available at http://www.maawg.org/system/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf.; *see also* MAAWG Comments on "Cybersecurity, Innovation and the Internet Economy June 2011," (July 2011), available at http://www.maawg.org/sites/maawg/files/news/MAAWG_DoC_Internet_Task_Force-2011-08.pdf.

deterring botnet threats. Botnet attacks pose a threat to nearly all layers of the Internet. While they typically do not target disruption of the physical transmission layer of the Internet, since bot masters usually are interested in purloining transaction data and information from businesses and end-users that are interacting with the networks, they can be used in Distributed Denial of Service attacks to orchestrate disruption of websites for such purposes as extortion or exerting political influence. End-users, and the companies that manufacture products for them, must therefore play an active role in the prevention of botnet infection. In its Best Practices Report, MAAWG specifically identified a number of "infection vectors," or points of vulnerability, most of which are located close to the end-user. These include un-patched operating systems, software vulnerabilities, weak or non-existent passwords, malicious Web sites, un-patched browsers, malware and social engineering techniques to gain access to the user's computer.[14]

As the RFI correctly notes, "other entities beyond ISPs (such as operating system vendors, search engines, security software vendors, etc.) can participate in anti-botnet related efforts."[15] To this end, MAAWG's anti-botnet activities include input from operating system vendors, e-commerce platforms, social networks, search engine operators, web portals, device manufacturers, software developers, security vendors, applications and tool providers, and wireless network operators – as well as from traditional ISPs. The Departments should take steps to help coordinate public-private and inter-industry groups working on anti-botnet initiatives and to promote a holistic, multi-layered approach to combating botnets, incorporating input from all segments of the broadband ecosystem.

---

[14] *Best Practices Report* at 3.

[15] RFI, 76 Fed. Reg. at 58469.

II. THE DEPARTMENTS SHOULD NURTURE AND BUILD UPON EXISTING EFFORTS AND INITIATIVES AIMED AT COMBATING BOTNETS AND RESIST IMPOSING PRESCRIPTIVE MANDATES AND TOP-DOWN DIRECTIVES

NCTA's members share the Departments' concerns regarding the need to take affirmative measures to combat the growing risks to cybersecurity presented by botnets. Many of the necessary measures and efforts are already well underway. With their strong incentives to provide subscribers with a secure network environment, cable operators are already providing their subscribers with the means to protect themselves from botnet attacks and safeguard their financial, transactional, and other sensitive information from cyber theft. Other ISPs and broadband service providers are undertaking similar initiatives. Cable companies also share with other providers of services across the Internet ecosystem a responsibility and commitment to protect and promote cybersecurity and are, to that end, actively engaged in a number of important inter-industry initiatives and public-private partnerships that are helping in the fight against botnet threats.

Government policy should continue to encourage and nurture the type of consumer-facing and inter-industry anti-botnet initiatives already undertaken by cable and others in the private sector. A number of the ideas and measures referenced in the RFI clearly warrant further consideration. Some are already being implemented in various ways by ISPs and other broadband service providers. To ensure an effective and efficient response to the problems raised by botnets, the Departments' efforts in this area should supplement and complement – and not substitute for or replace – ongoing industry initiatives and programs.

First, NCTA fully agrees that promoting data sharing on botnet threats, attack signatures, mitigation tactics and remediation strategies is a key element of an effective anti-botnet policy. NCTA supports initiatives to encourage and enhance cooperation and information sharing

between all relevant parties from both the public and private sectors that have a stake in the fight against botnets. NCTA agrees with the Business Roundtable's finding that "[n]either the government nor private-sector companies have adequate information on the most consequential cybersecurity risks facing our nation."[16] Managing today's cyber threats "requires a robust environment for sharing information between the public and private sectors as well as among firms within the private sector," yet "[o]ur domestic public policy environment has not evolved to provide an integrated and dynamic approach to cybersecurity risk management."[17] The open and voluntary exchange of information and ideas is critical to addressing the diverse and ever-changing threats that challenge our cybersecurity. NCTA's experience in the fight against spam and viruses has shown that collaboration and industry cooperation enhances the efforts of all stakeholders.

Rather than divert time and resources into developing new or parallel entities, however, the Departments should first make every effort to leverage the existing expertise and organizational infrastructure of groups such as CSRIC, MAAWG, and NSTAC that are already involved in developing innovative and effective tools and strategies for combating botnets. As noted above, a key feature of that effort is to ensure that all segments of the broadband ecosystem, and not just ISPs, are engaged and committed to this objective.

Further, effective information sharing not only requires the participation of all affected stakeholders, but it is also enhanced by reliance upon shared terminology and common metrics. Because botnet problems are relatively recent phenomena, there is still not a common understanding of basic metric concepts, such as how to measure the size and duration of a botnet

---

[16] Business Roundtable, *Mission Critical: A Public-Private Strategy for Effective Cybersecurity*, at 6 (October 2011), *available at* http://www.scribd.com/doc/68270292/Mission-Critical-A-Public-Private-Strategy-for-Effective-Cybersecurity.

[17] *Id.*

attack, or how to ascertain when an infection has been remediated. The Departments may be able to help facilitate and accelerate the important process of adopting common metrics for purposes of data analysis by convening meetings of key stakeholders so that a consensus terminology can be developed and relied upon by all interested parties.

MAAWG is engaged in a comprehensive effort to develop a program that will gather true cross-ISP bot infection metrics. The MAAWG metrics will help scope the size of the problem, and measure the success of the industry's efforts to combat it. The Departments should look for ways to support this ongoing effort, which can foster a number of benefits.

One of the suggestions discussed in the RFI is the creation of a centralized consumer resource center that would provide technical support to end-users. Under the proposal, the resource center would be supported by a wide number of players, pooling resources from both the public and private sector. While a resource center may be useful for small ISPs that might lack the resources needed to adequately assist their subscribers in dealing with bot attacks, making participation a requirement could inadvertently harm anti-botnet efforts by deterring incentives of individual ecosystem participants to invest in cybersecurity technology and disrupting a service provider's relationship with its customers.

Another danger associated with creating a single centralized resource facility is that the development of deterrence and detection measures that are uniform across multiple providers can allow bot masters to launch an attack on multiple networks simultaneously if they are able to circumvent those measures. Such an attack is a trivial process for bot software developers. By contrast, botnet attacks will be harder to initiate or perpetuate where bot masters are forced to confront different strategies and tools from a variety of network providers and tool vendors. For all these reasons, any resource center should work in concert with ongoing customer-facing anti-

botnet efforts and initiatives, and not displace those efforts or become a mechanism for top-down policy prescriptions or uniform responses to botnet threats.

While the cable industry sees potential value in a centralized resource center as a mechanism for the exchange of ideas and information, existing entities such as MAAWG and the Anti-Phishing Work Group ("APWG") have already developed strong working relationships to facilitate the exchange of ideas across the entire technology industry. Independent associations like MAAWG and APWG also have the advantage of existing relationships with international stakeholders, an essential element of combating a threat that is not constrained by geographic boundaries. At this point in time, it may make more sense for the Departments to determine how best to leverage these existing models rather than attempting to reinvent the wheel by creating an entirely new entity.

Second, with respect to detection and notification, it is particularly important that ISPs and other broadband service providers be afforded maximum flexibility to develop and implement anti-botnet practices and protocols that are tailored to their particular network and business model characteristics. The risks associated with adopting standards or government-sponsored codes of conduct is that they inhibit innovation and divert resources toward checklist compliance and away from individualized solutions tailored to a provider's particular network and circumstances. As the WG 8 reported, "[t]he Working Group specifically did not undertake to make any recommendations of any measures for which it should be mandated that service providers implement. In light of the complexity and diversity of individual networks, and the

fast changing nature of the botnet security threats, individual networks should be able to respond to security threats in the manner *most appropriate for their own network.*"[18]

Competitive incentives have led to the development of a number of diverse approaches to internet security, and companies are continuing to adapt to new challenges as they arise. It is essential that any effort on the part of the government to facilitate the further development of internet security does not impede the private sector's flexibility to address ever-changing threats. At this stage of the battle against botnets, the best policy response is to encourage and promote the diversity and variety of responses that will arise from affording private stakeholders the freedom and flexibility to develop responses and practices that optimize their own particular resources and strengths.

The emergence of offerings such as Comcast's Constant Guard Security Suite, Cox's Security Suite Plus Powered by McAfee, Charter's Security Suite, and similar programs by other cable operators as discussed above, exemplifies the value and utility of reliance upon best practices and flexible, market-based tools (in contrast to prescriptive rules) to address botnet threats. Hence, NCTA believes that the government's focus should principally be on helping to develop best practices and facilitating voluntary standardization efforts, and not on imposing prescriptive mandates or adopting a government-sponsored code of conduct.

Today, cable operators employ a variety of practices and tools to detect botnet and malware threats, including analysis of Internet traffic for IP addresses of known malicious hosts and botnet command and control centers, as well as notifications from trusted third-parties (*e.g.*, network equipment vendors or security specialists such as Damballa) offering information on botnet signatures, fingerprints and hosting patterns and practices. Likewise, the use of deep

[18] *Internet Service Provider (ISP) Network Protection Practices*, at http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf. (emphasis added).

packet inspection (DPI) for botnet protection and prevention purposes could provide some advantages and benefits depending upon the nature of the threat and the breadth and pace of its proliferation within a network. It is only a matter of time before developers of bot software create programs designed to evade detection efforts that rely on technologies that are currently employed by some cable operators. The strategies and tactics of botnet perpetrators are constantly evolving, quickly obsolescing prevention and mitigation techniques. In this circumstance, it makes no sense to restrict or exclude utilization of any technology or tool that can effectively address botnet risks and attacks.

Finally, the RFI asks if express liability protection would provide greater incentives to companies to undertake anti-botnet activities.[19] Whether such protections would incentivize further private sector activity is certainly an issue that merits further exploration and study.

In the context of broader cybersecurity policy, it is widely recognized that the objective of inter-industry and industry-government information sharing on actual or potential cyberattacks potentially conflicts with statutory provisions, including the Electronic Communications Privacy Act ("ECPA"), the Freedom of Information Act, antitrust restrictions on intercompany sharing of proprietary information, and privacy provisions in the Communications Act. The uncertainty over the applicability of these laws to cybersecurity efforts, including botnet remediation, can create procedural impediments to the timely sharing of relevant information. They also can hamper robust information sharing, as companies grapple with, for example, whether sharing email headers or signature information embedded in content associated with a particular botnet, implicates issues under ECPA or privacy laws.

[19] RFI, 76 Fed. Reg. at 58468, 58469.

If the goal is to promote real-time and robust information sharing, the Departments should examine closely the extent to which existing statutes are inhibiting attainment of that objective. NCTA agrees that industry and government must remain alert to their potential to constrain such efforts and be prepared to address such constraints as they arise.

CONCLUSION

NCTA commends the Departments for their leadership in focusing attention and resources on the importance of efforts to detect, deter, and remediate botnet threats. The Federal government should ensure that cable operators and other broadband service providers are afforded the flexibility and freedom to develop and implement anti-botnet practices and protocols that are tailored to their particular network and business model characteristics. Prescriptive rules would needlessly constrain effective and real-time response measures. The government has an important role to play, however, in supporting the anti -botnet efforts and initiatives undertaken by ISPs, other Internet ecosystem participants, inter-industry organizations, and public-private partnerships. The government can also facilitate anti-botnet efforts by taking steps to ensure that existing statutory provisions, such as ECPA, various privacy statutes, antitrust restrictions and other laws do not inhibit robust and timely sharing of information on botnet threats and remediation measures.

Respectfully submitted,

/s/ Rick Chessen

William Check, Ph.D.
Senior Vice President
Science & Technology
And Chief Technology Officer

Rick Chessen
Neal M. Goldberg
Loretta P. Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W., Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

November 14, 2011