

Table of Contents

- I. GUIDING PRINCIPLES FOR A FLEXIBLE, RESPONSIVE AND VOLUNTARY FRAMEWORK TO ADDRESS THE BOTNET THREAT 2**
- II. PUBLIC-PRIVATE PARTNERSHIPS ARE PROACTIVELY ADDRESSING SECURITY ISSUES RELATING TO BOTNETS..... 5**
- III. THE DEPARTMENTS SHOULD PROMOTE EFFORTS THROUGH EXISTING FRAMEWORKS TO HELP FORMULATE VOLUNTARY MEASURES FOR ADDRESSING ILLICIT USE OF COMPUTER EQUIPMENT BY BOTNETS AND RELATED MALWARE 8**
- IV. MULTIPLE ISSUES MUST BE CONSIDERED WHEN EXAMINING PREVENTION, DETECTION, NOTIFICATION AND REMEDIATION MEASURES. 11**
 - A. USTelecom’s Members are Actively Engaged in Prevention of Botnet Infections.... 11**
 - B. Subject to Certain Legal and Pragmatic Limitations, Various Methods are Available for Bot Detection. 13**
 - C. Notification Mechanisms Can Play an Important Role in the Remediation of Botnets and Should be Voluntarily Utilized by all Internet Stakeholders. 14**
 - D. ISPs Should be Afforded Broad Flexibility in Adopting and Implementing Remediation Efforts, and any Pooled Remediation Resource Should be Optional for Service Providers. 18**
- V. CONCLUSION 19**

* * *

**Before the
Department of Commerce
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 TELECOM ASSOCIATION**

USTelecom¹ provides these comments to the Department of Commerce (Commerce) and the Department of Homeland Security (DHS) (collectively “the Departments”) in the above referenced proceeding,² regarding the requirements for, and possible approaches to creating, a voluntary industry code of conduct to address the detection, notification and mitigation of botnets. USTelecom shares the Departments’ concerns over the potential economic impact of botnets and the problems they cause to computer systems, businesses, and consumers. As the Departments consider the development of a voluntary approach to the botnet threat, it is imperative that their efforts be informed through guiding principles that will lead to the development of an effective, flexible and responsive framework.

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

² Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, 76 Fed. Reg. 58,467 (September 21, 2011) (*Notice*).

I. GUIDING PRINCIPLES FOR A FLEXIBLE, RESPONSIVE AND VOLUNTARY FRAMEWORK TO ADDRESS THE BOTNET THREAT

In their Notice, the Departments detail the numerous problems resulting from the proliferation of botnets and malware throughout the entire Internet ecosystem. Originally viewed as a nuisance to consumers, botnets and malware have in recent years become powerful weapons used by organized crime and hostile nations to disseminate spam, store and transfer illegal content, and attack the servers of government and private entities with distributed denial of service attacks. They are increasingly being used to obtain classified government information and industry secrets.³

Given the profound threat of botnets to a broad range of areas – including privacy, network security and national security –any response by the Departments to the botnet threat must be thorough, flexible and responsive. In this regard, certain guiding principles should be considered by the Departments as they contemplate solutions to this threat.

First, because of the broad and diverse nature of the Internet ecosystem, any public-private effort geared towards a single solution or discrete industry segment should be rejected. Such an approach would be the equivalent of a modern-day Maginot Line – a formidable single line of defense that creates the illusion of security, but is easily circumvented. For this reason, USTelecom supports the Departments facilitating a discussion about the potential for collective industry and government action to identify holistic solutions to improve the security of computer networks for consumers, industry and the government. The Departments should therefore convene a dialogue that includes participants from across the Internet ecosystem, including Internet service providers (ISPs), software developers, search providers and government

³ Testimony of Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C., April 12, 2011.

agencies. In order to be effective, any voluntary response plan should broadly cover strategies for educating consumers, identifying security threats and notifying end users, and must entail remediation efforts that leverage the capabilities of all participants in the value chain.

Second, because of the organic and rapidly changing nature of the botnet threat, any framework that the Departments implement must be flexible and responsive. Moreover, given the nature of the numerous stakeholders within the Internet ecosystem, there can be no ‘one-size-fits-all’ answer. Rather, proposed solutions must be tailored to the different participants in the ecosystem, given their different business models and access to resources.

Third, any coordinating efforts considered by the Departments must be voluntary in nature. Such voluntary approaches ensure a more collaborative environment for all stakeholders, which is essential in the rapidly changing botnet environment. The benefits of such collaborative efforts can be seen in the numerous instances where voluntary efforts have led to successful outcomes.

Fourth, one of the most critical effective roles that could be played by the Federal government is through implementation of information sharing and awareness programs. Such efforts complement additional mechanisms for addressing the botnet issue. For example, information sharing enhances the flexible and responsive framework discussed above, by providing stakeholders with real-time information to effectively respond to new botnet threats. In addition, the collaborative environment created by a voluntary framework fosters the relationships that are essential to effective information sharing.

Finally, before implementing any framework, the Departments should validate its effectiveness through a data-driven analysis. Such an independent economic and fact-based analysis could be developed by the Departments to determine the costs associated with

implementing a voluntary code of conduct based on the variety of prevention, detection, notice and remediation options, and the varying characteristics of ISPs such as differing business models, economies of scope and scale, and position in the ecosystem. The study should also attempt to validate the benefits associated with existing programs and the ability of these initiatives to produce material and sustainable benefits to the ecosystem at large. Any study should also examine the roles and contributions of members in the broader internet ecosystem and the effectiveness of government programs that have been implemented in other nations (*e.g.*, Australia, Japan, and Germany).

Indeed, the SANS Institute has already filed comments in this proceeding that discuss its analysis of the “actual experience of ICode in Australia.”⁴ The ICode is an initiative undertaken by the Australian government to deliver a standard set of best practices for ISPs to follow to preserve the integrity of their networks.⁵ The SANS Institute filing concludes that the desired impact of the program – a “significant reduction of the number of bots in each of the ISPs that participated” – was “not gained.”⁶ The SANS Institute went on to note that in order for any similar effort undertaken by the United States to “be credible” would need to “demonstrate how the US version would get substantial reductions” in the number of bots, with a 50% reduction being the “sensible target for a national initiative.”⁷ The stark findings contained in the SANS Institute filing illustrate both the severity of the problem, and the critical need to validate effectiveness of any program through a data-driven analysis prior to its implementation.

⁴ *See*, Comments of the SANS Institute in response to the *Notice* (submitted November 4, 2011) (*SANS Institute Comments*).

⁵ *See*, Internet Industry Association website (available at: <http://www.iiia.net.au/index.php/all-members/869-get-ready-for-icode-in-force-1-december-2010.html>) (visited November 10, 2011).

⁶ *SANS Institute Comments*.

⁷ *Id.*

II. PUBLIC-PRIVATE PARTNERSHIPS ARE PROACTIVELY ADDRESSING SECURITY ISSUES RELATING TO BOTNETS

The botnet dilemma is a highly complex issue that impacts a global set of stakeholders representing public and governmental entities. In such a complex environment, it would be impossible for a single sector or specific group of stakeholders (*e.g.*, ISPs or government entities) to successfully implement a response. Only through cooperation and ongoing coordinated efforts can critical goals be successfully attained. Such a cooperative approach has been consistently identified by many key organizations as an essential component of the nation's cybersecurity strategy.⁸

Fortunately, there is an established history of success under such cooperative models.⁹ In particular, the Departments should acknowledge the success of voluntary public-private efforts

⁸ See *e.g.*, Center for Strategic and International Studies Report, Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, December 2008, pp. 43 – 48 (stating that the U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities) (*CSIS Report*) (available at: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf) (visited November 3, 2011); see also, White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. iv (stating that the Federal government should enhance its partnership with the private sector) (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited November 3, 2011) (*White House Cyberspace Policy Review*); see also, Intelligence and National Security Alliance Report, *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*, November 2009, p. 3 (stating that an effective public-private partnership for cyber security would provide the abilities to detect threats and dangerous or anomalous behaviors, to create more secure network environments through better, standardized security programs and protocols and to respond with warnings or technical fixes as needed) (available at: <http://insaonline.org/assets/files/CyberPaperNov09R3.pdf>) (visited November 3, 2011) (*INSA Cyber-Security Report*).

⁹ Outside of the botnet context, there has been a long and successful track record of public-private partnerships. According to the National Council for Public-Private Partnerships (Council), public-private partnerships have been in use in the United States for over 200 years and “thousands are operating today.” See The National Council for Public-Private Partnerships website, Top Ten Facts About PPPs, (available at: <http://ncppp.org/presskit/topten.shtml>) (visited November 3, 2011). Of particular note, the Council states that such partnerships are not only extremely common and an essential tool during challenging economic times, but they also often

already underway through various organizations, including DHS's National Infrastructure Protection Plan, the 2011 National Sector Risk Assessment for Communications, and the recently formed Supply Chain Task Force. Another example can be found in the Communications Security, Reliability and Interoperability Council's (CSRIC) at the Federal Communications Commission (FCC).¹⁰ Since its initial establishment in 2009, the CSRIC has established working groups that specifically focused on ISP Network Protection Practices and Cyber Security Best Practices, as well as a more recent working group to address Botnet Remediation.

Over the past several years, organizations such as these have been working diligently to provide recommendations for ensuring optimal security and reliability of communications systems.¹¹ Combined, these working groups have identified dozens of new and modified best

lead to better public safety. *Id.* On the issue of public safety, the Council notes that “[f]rom Los Angeles to the District of Columbia, local governments have formed creative partnerships with private companies to enhance the safety of its streets and its citizens. By turning over the operation of parking meters or the processing of crime reports to private-sector partners, police officers can spend more time on the streets doing the jobs for which they are trained. This is particularly important as Home Land Security has risen as a concern for many.” *Id.*

¹⁰ CSRIC members represent a diverse and balanced mix of viewpoints from public safety organizations; Federal, state and local government agencies; the communications industry; organizations representing Internet users; utility companies; public interest organizations; and other recognized experts. *See*, Public Notice, *FCC Announces Membership of the Communications Security, Reliability, and Interoperability Council*, DA 11-1321, 26 FCC Rcd 10973 (released August 8, 2011).

¹¹ For example, the FCC has established CSRIC Working Group 7, which is specifically focused on the botnet threat, and is tasked with “propos[ing] a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs.” *See*, CSRIC III Working Group Descriptions and Leadership (available at: <http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions.pdf>) (visited November 4, 2011) (*CSCRIC III Descriptions*). Building on the work of previous working groups, the new Working Group 7 – which includes representatives from the federal government, the ISP community (including USTelecom), edge providers such as PayPal, software developers and Internet security experts –will pinpoint potential ISP implementation obstacles to the previously adopted botnet remediation practices and identify steps the FCC can take that may help overcome these obstacles. It will also identify performance metrics to evaluate the effectiveness of previous

practices to address protection for end-users as well as the network from the botnet threat¹² and other cyber vulnerabilities.¹³

In addition, industry sponsored organizations, such as the Internet Engineering Task Force (IETF) and the Messaging Anti-Abuse Working Group (MAAWG), have been working to develop consensus-based solutions to the botnet issue.¹⁴ For example, the MAAWG, an industry group with global members companies from Asia, Europe, North America and South America, is working on a variety of initiatives addressing ongoing and emerging messaging abuse issues, including bot mitigation. In fact, the MAAWG is the only organization that targets messaging abuse by simultaneously focusing on the varied facets of the *international* challenge, and organizes its committees around technology, industry collaboration, cooperative public policy

working group efforts designed to curb the spread of botnet infections. *CSCRIC III Descriptions*, p. 6. CSRIC Working Group 7 has also proposed developing an initial ISP code of conduct by January 2012/March 2012.

¹² Final Report, CSRIC Working Group 8, *Internet Service Provider (ISP) Network Protection Practices*, December 2010 (available at: http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf) (visited October 27, 2011) (*CSRIC Working Group 8 Final Report*). The report was produced and issued during the second assembly of the CSRIC II, which was chartered between March 19, 2009 and March 18, 2011. See, FCC website, *Communications Security, Reliability and Interoperability Council II* (available at: <http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-ii>) (visited October 27, 2011).

¹³ See e.g., *DHS National Infrastructure Protection Plan*, 2009, p. 12 (available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) (visited November 14, 2011) (discussing ways to both reduce the cybersecurity risk and enhance cybersecurity); see also, *DHS Communications Sector-Specific Plan*, 2010, p. i (available at: <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf>) (visited November 14, 2011) (discussing how the Communications Sector can manage risk utilizing both public and private resources, how partners can implement programs and practices to achieve sector goals, and how the sector can measure the success of protective activities.); see also, *CSRIC Working Group 2A Report*, p. 16.

¹⁴ See, IETF website (available at: <http://www.ietf.org/about/>) (visited October 25, 2011). The IETF is a large, open and voluntary international community of network designers, operators, vendors, and researchers “concerned with the evolution of the Internet architecture and the smooth operation of the Internet.” See, MAAWG website (available at: <http://www.maawg.org/>) (visited November 14, 2011).

efforts and special interest groups. The technical work of groups such as the MAAWG and the IETF are accomplished through its working groups.¹⁵

Whether through industry-led programs or public-private initiatives, these types of cooperative efforts are widely embraced by government and industry alike.¹⁶ The Departments should encourage such initiatives and, where feasible, constructively participate in their work.

III. THE DEPARTMENTS SHOULD PROMOTE EFFORTS THROUGH EXISTING FRAMEWORKS TO HELP FORMULATE VOLUNTARY MEASURES FOR ADDRESSING ILLICIT USE OF COMPUTER EQUIPMENT BY BOTNETS AND RELATED MALWARE

To the extent the Departments seek to expand their involvement in identifying solutions to the botnet problem, USTelecom recommends that that the Departments fulfill their collective desire to coordinate with all key stakeholders to ensure that they are not “duplicating any efforts

¹⁵ The MAAWG recently published a draft paper entitled “Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks.” Messaging Anti-Abuse Working Group, Paper, Nirmal Mody, Michael O’Reirdan, *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks* (available at: http://www.maawg.org/system/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf) (visited November 10, 2011) (*MAAWG Paper*). The MAAWG Paper contains a detailed discussion on issues relating to botnet infections, and includes a review of the methods that ISPs may employ in an effort to minimize the effects of computers used by their subscribers, which have been infected with malicious bots. The MAAWG Paper acknowledges that its recommendations are “not intended to be the ultimate solution for all types of bots,” and because the bot threat is “constantly evolving,” the recommendations are meant to be “generic yet scalable to grow with the challenge.” *MAAWG Paper*, p. 2.

¹⁶ As DHS Secretary Janet Napolitano concluded in a speech on cybersecurity issues, “[t]o be most effective, we in government must work closely with the private sector, and include it in our work as a full partner from the very start.” Secretary’s Web Address on Cybersecurity, *A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack*, October 20, 2009 (available at: http://www.dhs.gov/ynews/gallery/gc_1256070988236.shtm) (visited November 3, 2011) (*Napolitano Speech*). President Obama framed his Administration’s policy more emphatically, when he stated, “[s]o let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.” Cross Sector Cyber Security Working Group, Incentives Subgroup, *Incentives Recommendations Report*, September 2009, p. 6 (*CSCSWG Report*).

for industry or government.”¹⁷ In the Notice, Commerce in particular states its desire to “expand its role of working with multiple stakeholders to facilitate and promote the use of voluntary codes of conduct.”¹⁸ Moreover, any such coordinating efforts must be voluntary in nature, thereby ensuring a more collaborative environment for all stakeholders.

The Federal government can and should play an important role in coordinating voluntary efforts by all Internet stakeholders to address the scourge of botnet infections. The Departments in particular are ideally suited to fulfill this role, in addition to spearheading efforts related to consumer outreach and education, and supporting critical research in this area.

First, the Departments, working in partnership with all Internet stakeholders, can develop strategies to promote cybersecurity awareness and education and increase innovation. This should start with broad education for all stakeholders on the need for good cybersecurity. At the same time, increasing consumer awareness and education can help drive market demand for security services, such as additional consumer tools, which may or may not involve notification. In this regard, the Notice appropriately acknowledges the “essential role” that DHS in particular has played in building cybersecurity educational programs for consumers.¹⁹

In previous proceedings, USTelecom has expressed strong support for governmental outreach efforts.²⁰ Such an approach can have a tangible and positive impact on the nation’s cybersecurity, and was previously identified by the White House as a near-term action plan in its

¹⁸ Notice, p. 58467.

¹⁹ *Id.*, p. 58467. The Notice points out that DHS’s educational programs “emphasize that every Internet consumer has a role to play in securing cyberspace and in ensuring the safety of ourselves, our families, and our communities online.” Notice, p. 58467. The Notice highlights the various DHS outreach programs, including its National Cybersecurity Awareness Month and Campaign, as well as its Awareness Campaign “Stop. Think. Connect.” *Id.*

²⁰ Comments of USTelecom at the FCC, *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan, NBP Public Notice # 8*, pp. 17 – 19, GN Docket Nos. 09-47, 09-51, 09-137 (submitted November 12, 2009).

2009 Cyberspace Policy Review.²¹ Targeted outreach, particularly to the consumer and small business communities, can be coordinated through broader federal government public policy campaigns. The Federal government has a long track record of tremendously successful outreach in other areas,²² and such an approach is ideally suited for informing consumers and small businesses about critical issues relating to botnets.²³

Second, government is ideally suited to sponsor research on the effectiveness of anti-botnet programs. All parties should support a data-driven approach. While the Commerce RFI notes that many security experts agree that notification is one tool that has proven effective in reducing the rate of botnet infection, they offer no evidence to support that claim. Also the foreign governments and private-sector companies that have introduced similar programs have not offered any publicly available data to prove the effectiveness of their programs. While there

²¹ See White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 37 (identifying as a near term action plan the initiation of a national public awareness and education campaign to promote cybersecurity).

²² For example, the Ad Council has highlighted the success of many of its public awareness campaigns, which it notes have been “raising awareness, inspiring action and saving lives for more than 70 years.” See, Ad Council website (available at: <http://www.adcouncil.org/About-Us>) (visited November 4, 2011). The impact of various government campaigns can be seen across a wide variety of issue areas. Forests destroyed by wildfires decreased substantially – from 22 million acres to less than 8.4 million acres per year -- since the Forest Fire Prevention campaign began See, Ad Council website (available at: <http://www.adcouncil.org/Our-Work/The-Classics/Forest-Fire-Prevention>) (visited November 4, 2011). In the area of drunk driving prevention, the Ad Council notes that its ongoing efforts have had a substantial effect in the area of public awareness and measurable results. See, Ad Council website (available at: <http://www.adcouncil.org/Impact/Case-Studies-Best-Practices/Drunk-Driving-Prevention>) (visited November 4, 2011). In addition, safety belt usage has increased from 14% to 79% since the Safety Belt campaign launched in 1985 -- a change that is estimated to have saved 85,000 lives, and \$3.2 billion in costs to society. See, Ad Council website (available at: <http://www.adcouncil.org/Our-Work/The-Classics/Safety-Belt-Education>) (visited November 4, 2011).

²³ See e.g., Comments of USTelecom, September 20, 2010, pp. 6 – 7, (submitted to the Department of Commerce in response to, *Cybersecurity, Innovation and the Internet Economy*, 74 Fed. Reg. 44,216, (July 28, 2010)).

have been some initial independent studies attempting to validate the effectiveness of these programs, no definitive empirical evidence has yet been made available.

IV. MULTIPLE ISSUES MUST BE CONSIDERED WHEN EXAMINING PREVENTION, DETECTION, NOTIFICATION AND REMEDIATION MEASURES

As the Notice acknowledges, there is no panacea that would guarantee complete protection against the botnet threat. This acknowledgement is further underscored by the findings contained in the filing of the SANS Institute. As a result, Internet stakeholders implement a series of independent, but related, measures to ensure sufficient security of the networks and its users. These measures typically include prevention, detection, notification and remediation, although each category is subject to certain challenges and limitations. The efforts of USTelecom's members in these areas are addressed below.

A. USTelecom's Members are Actively Engaged in Prevention of Botnet Infections

The Departments seek information on preventative measures that are most effective in stopping botnet infections.²⁴ USTelecom's member ISPs actively monitor and manage the performance of their networks. Should they identify anomalous traffic or conditions, they respond accordingly. Through the ongoing work of a variety of security organizations, member ISPs stay informed about the latest botnet/malware techniques.²⁵ Other widely implemented

²⁴ Notice, p. 58468.

²⁵ See, CSCRIC Working Group 8 Member List (available at: <http://transition.fcc.gov/pshs/advisory/csrc/wg-8-members.pdf>) (visited October 27, 2011). For example, the Botnet Remediation Business Practices developed by CSCRIC Working Group 8 include 24 best practices geared specifically towards prevention measures by ISPs. It is important to note that these best practices were developed with input from a broad range of Internet stakeholders, including Federal government representatives, public interest groups and non-ISP companies such as Google, Microsoft and Symantec. The best practices contained in the Botnet Remediation Business Practices cover various efforts that range from customer education through more technical measures.

prevention methods by USTelecom members include protection of DNS servers, and maintaining methods to detect bot and malware infection. For example, some companies have implemented – and provide as stand-alone offerings – various forms of intrusion and detection services. These tools generate alerts and record suspicious events throughout the network and can provide immediate corrective responses that stop or alleviate malicious attacks.

USTelecom members also offer their subscribers a wide variety of tools in conjunction with their internet access services such as anti-virus software that can help subscribers scan their machines to identify threats. And some USTelecom members are actively notifying their subscribers today if they are suspected to be infected with a botnet, in particular in regards to large-scale threats, and are experimenting with a variety of tools that may help consumers determine if they have been communicating with known botnet command and control hosts which would indicate a high likelihood of infection.

Nevertheless, ISPs recognize that the first line of defense against the threat of botnet infections involves effective, implementable prevention measures, and their main focus is on how they can help residential broadband end-users prevent bot malware infections from occurring in their devices and networks. In addition to providing firewall and anti-virus services, many ISPs provide or support third-party tutorial, educational, and self-help resources for their customers to educate them on the importance of safe computing practices,²⁶ and many of USTelecom's member companies are at the forefront in this area.²⁷ In previous proceedings at the FCC, USTelecom has highlighted its member companies' efforts with respect to consumer

²⁶ See e.g., *CSRIC Working Group 8 Final Report*, p. 16.

²⁷ See e.g., AT&T Smart Controls website (available at: <http://www.att.net/smartcontrols-IncreaseSafety>) (visited October 27, 2011); see also, Verizon Security and Safety Center (<http://verizonsafeguards.com/>) (visited October 27, 2011).

outreach and education.²⁸ Moreover, USTelecom and its member companies are actively engaged in third-party outreach to consumers, through such organizations as the Family Online Safety Institute.

B. Subject to Certain Legal and Pragmatic Limitations, Various Methods are Available for Bot Detection

Detection of botnets can be accomplished through multiple means by the broad range of Internet stakeholders. Due to the dynamic and rapidly changing nature of botnet infections, it is imperative that broad industry collaboration and conversations are employed to identify the best tools and approaches that can be used for detection by all Internet stakeholders, including ISPs. Because a multi-faceted approach is ideal for addressing bot infections, the Departments should encourage broad consideration of these available tools and, in an ideal scenario, encourage a combination of approaches (*e.g.*, use of third-party tools and internal analysis).

In identifying the available mechanisms and tools, however, the Departments should acknowledge their limitations. For example, concerns have been raised that the current stable of available technical solutions are, “relatively immature, and are likely to change over time, evolving rapidly in the coming years.”²⁹ Moreover, available measures for botnet detection, notification and remediation in no way guarantee the remediation of all bots.³⁰ As a result, bot removal may “frequently be unsuccessful, or only partially successful, leaving the user's system

²⁸ See *e.g.*, Comments of USTelecom at the FCC, *Cyber Security Certification Program*, pp. 7 – 17, PS Docket No. 10-93 (submitted July 12, 2010); Comments of USTelecom at the FCC, *National Broadband Plan Recommendation To Create A Cybersecurity Roadmap*, pp. 4 – 10, PS Docket No. 10-146 (submitted September 23, 2010).

²⁹ Internet Engineering Task Force Paper, J. Livingood, M. O’Reirdan, *Recommendations for the Remediation of Bots in ISP Networks*, p. 10 (available at: http://datatracker.ietf.org/doc/draft-oreirdan-mody-bot-remediation/?include_text=1) (visited October 25, 2011) (*IETF Paper*). Despite the focus of the *IETF Paper* on an ISP-centric solution, USTelecom maintains that any public-private effort geared towards a single solution or discrete industry segment should be rejected.

³⁰ *Id.*, pp. 7 – 8.

in an unstable and unsatisfactory state or even in a state where it is still infected,” with side effects ranging from a loss of data to partial or complete loss of system usability. In fact, it can often be the case that the only way a user can be certain to have removed some of today's increasingly sophisticated malware is “by ‘nuking-and-paving’ the system.”³¹

Moreover, the current crop of available measures can sometimes be constrained by concerns relating to consumer privacy. As a result, when attempting to detect botnets on a user's system, ISPs may need to ensure that any Personally Identifiable Information (PII) collected or incidentally detected is properly protected.³² These concerns are further complicated by the fact that definitions for PII vary “from one jurisdiction to the next so proper care should be taken to ensure that any actions taken comply with legislation and good practice in the jurisdiction in which the PII is gathered.”³³

C. Notification Mechanisms Can Play an Important Role in the Remediation of Botnets and Should be Voluntarily Utilized by all Internet Stakeholders

USTelecom applauds efforts to curtail malware and believes that consumer notification represents just one important aspect of these efforts. The Notice, however, inappropriately suggests that ISPs may be best suited for addressing this issue, since they have “contact information for the end-user and a pre-existing relationship.”³⁴ The pervasiveness of the botnet problem represents a threat to the broad range of stakeholders throughout the entire Internet ecosystem. Therefore, USTelecom does not believe that notification responsibility should be presumptively assigned to ISPs for a variety of reasons.

³¹ *Id.*, p. 8. ‘Nuking and paving’ a computer involves reformatting the drive, reinstalling the operating system and applications (including all patches) from scratch, and then restoring user files from a known clean backup.

³² *Id.*, p. 10.

³³ *IETF Paper*, p. 10.

³⁴ *Notice*, p. 58467.

First, instances involving botnet infections have occurred involving all manner of devices and services, including iPods,³⁵ factory installed hard drives,³⁶ social networks,³⁷ and even digital picture frames.³⁸ A cyber policy review report issued by the White House in 2009, acknowledged this reality when it proposed a “broad, holistic approach to risk management,” given the “challenge with supply chain attacks.”³⁹ The pervasiveness of this problem demonstrates the broader nature of the threat to the entire Internet ecosystem. Moreover, many other members of the ecosystem maintain an equal amount of contact information for their users as do ISPs and have established strong relationships with their customers. For example, social

³⁵ Jonny Evans, Computer World, *Apple warns of Windows virus in latest video iPods*, Oct. 18, 2006 (available at: http://www.computerworld.com/s/article/9004234/Apple_warns_of_Windows_virus_in_latest_video_iPods) (visited Oct. 25, 2011).

³⁶ Greg Keizer, Computer World, *Update: Maxtor drives contain password-stealing Trojans*, November 12, 2007 (available at: http://www.computerworld.com/s/article/9046424/Update_Maxtor_drives_contain_password_stealing_Trojans?taxonomyName=security) (visited October 25, 2011).

³⁷ Graeme McMillan, March 23, 2011, Techland, *40% of Social Network Users Attacked by Malware*, March 23, 2011 (available at: <http://techland.time.com/2011/03/23/40-of-social-network-users-attacked-by-malware/>) (visited October 25, 2011) (*Techland Malware Article*).

³⁸ Greg Keizer, Computer World, *Best Buy sold infected digital picture frames*, November 12, 2007 (available at: http://www.computerworld.com/s/article/9058638/Best_Buy_sold_infected_digital_picture_frames) (visited Oct. 25, 2011).

³⁹ White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 34 (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited October 25, 2011) (*White House Cyberspace Policy Review*). The report noted that “a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover,” and that foreign manufacturing presents “easier opportunities for nation-state adversaries to subvert products.” The report went on to state that while counterfeit products have created the most visible supply problems, potential concerns are raised from “easier subversion of computers and networks through subtle hardware or software manipulations,” due to the emergence of new centers for manufacturing, design, and research across the globe. *White House Cyberspace Policy Review*, p. 34.

networking sites such as Facebook maintain extremely detailed information on their users.⁴⁰ In light of the fact that one recent study found that 40 percent of social network users had encountered malware attacks,⁴¹ social networking sites are critical stakeholders in the notification process. USTelecom maintains that any meaningful response to malware must be holistic in nature, and any effective approach must ultimately involve the broad range of Internet stakeholders.

Second, while there are numerous options available to ISPs and other equipment and service providers for notifying consumers of possible botnet infection, there are various drawbacks to the over-reliance on notification of consumers by ISPs, as noted by a variety of security organizations.⁴² For example, email notifications are not “guaranteed to be viewed within a reasonable time frame, if at all,” since the ISP’s or other stakeholder customers may be “using a different primary e-mail address than that which they have provided,” to their respective provider.”⁴³ Additionally, many consumers simply do not pay attention to e-mails from their providers, and, even if they are contacted they are “very likely to lack the necessary technical expertise to understand or be able to effectively deal with the threat.”⁴⁴ Other notification mechanisms, such as telephone calls or postal notification, suffer from similar drawbacks.⁴⁵

⁴⁰ For example, Facebook notes that it receives a “number of different types of information” about its users, including name, email address, birthday, and gender. *See*, Facebook Privacy website, <https://www.facebook.com/about/privacy/your-info#infoceived> (visited November 14, 2011). It also receives information regarding a user’s IP address, location, the type of browser they use, the pages they visit, as well as data it receives from its “advertising partners, customers and other third parties.” *Id.*

⁴¹ *Techland Malware Aritcle.*

⁴² *See generally*, IETF Paper, pp. 12 – 19. *MAAWG Paper*, p. 5.

⁴³ *IETF Paper*, pp. 12 – 13.

⁴⁴ *Id.*, p. 14; *MAAWG Paper*, p. 5.

⁴⁵ *IETF Paper*, p. 14.

Third, there are very real concerns that notices themselves could be exploited by cyber criminals since any available e-mail account may be already compromised by the bot.⁴⁶ Various security organizations have acknowledged that bot developers have impersonated the ISP or trusted sender and sent fraudulent emails to the users.⁴⁷ As a result, this spoofing technique of social engineering can often lead to new bot infestations. Moreover, if a user's email credentials are compromised, a hacker and/or a bot could simply access the user's email account and delete the email before it is read by the user. Even if an ISP resorts to a telephone call to the infected user, some bots may be able to disconnect, divert, or otherwise interfere with an incoming call.⁴⁸

Notification should be viewed by the Departments as one step in a series of necessary measures attempting to address bot infections. Absent sufficient remediation tools and procedures, notifications will not have the desired effect of adequately addressing the botnet problem. Moreover, the absence of appropriate remediation tools could easily lead to customer confusion and frustration for any stakeholder providing such notice to their customer. Therefore, any program should allow ISPs and other stakeholders the flexibility in how they help consumers address botnets. There are many approaches in the marketplace today, including e-mail notices, web portals or walled gardens. The key consideration is providing ISPs with the flexibility to experiment with and evaluate available options.

While the Departments state that many security researchers support notification as a means to reduce the prevalence of malware, and some countries have implemented programs such as what is contemplated, there is no evidence today to support that these programs have had a measurable impact on the prevalence of malware. USTelecom therefore supports broad

⁴⁶ *IETF Paper*, pp. 12 – 13; *MAAWG Paper*, p. 5.

⁴⁷ *IETF Paper*, p. 14.

⁴⁸ *Id.*

industry discussion regarding the various methods and most effective methods to provide notice to consumers. Because there are no effectiveness metrics or cost-benefit analyses of any of these measures, USTelecom strongly supports an independent study that examines these approaches in detail.

D. ISPs Should be Afforded Broad Flexibility in Adopting and Implementing Remediation Efforts, and any Pooled Remediation Resource Should be Optional for Service Providers

As detailed previously, ISPs offer consumers a wide variety of prevention capabilities to address infection of their computers by bots. Of course, once a bot has infected a consumer's computing device, remediation efforts may likely be necessary. At the outset, any Internet stakeholder, including ISPs, should be afforded the right to address remediation efforts with their customer by directing them to their specific remediation services.

To the extent the Departments deem it necessary to establish a centralized consumer resource center, however, certain considerations should be taken into account. First, any pooled resource center should be funded with government support. In the Notice, the Departments state that under this scenario, the government "would create a centralized resource to inform and educate consumers who have been notified that their equipment may be infected by a botnet."⁴⁹ USTelecom has previously stated in these comments that the Federal government can and should do more in terms of consumer education and outreach, and the pooled resource under this scenario could be a concrete step in this direction. Moreover, a government funded resource center would likely benefit many smaller ISPs. In particular, the availability of such a resource would benefit such ISPs who may lack the necessary capital resources to either fund their own remediation efforts, or be capable of contributing significantly to a solely private effort.

⁴⁹ Notice, p. 58468.

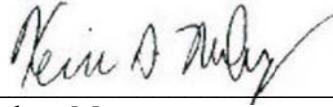
Second, any pooled resource center should be optional for ISPs. Given the established relationship between ISPs and their customers, many of the larger ISPs already have robust mechanisms in place to adequately address remediation efforts for their customers. Centralizing remediation efforts to a single entity would run the risk of confusing consumers, who would be forced to deal with an organization with which they may not be familiar. In addition, there is the added risk that consumers who have been notified of a bot infection by their ISP, and instructed to coordinate with the established resource center for remediation, would fail to do so. Given that rapid response to bot infections is essential, ISPs capable of adequate mediation responses must be afforded the opportunity to avoid unnecessary – and time consuming – steps.

V. CONCLUSION

USTelecom shares the Departments' concerns over the potential economic impact of botnets and the problems they cause to computer systems, businesses, and consumers. As the Departments consider the development of a voluntary approach to the botnet threat, it is imperative that their efforts be informed through certain guiding principles that include a voluntary, holistic, flexible and responsive approach to the botnet issue. Additionally, the Federal government can play a critical role in facilitating information sharing and awareness programs, and the effectiveness of any program should be evaluated prior to its implementation through a data-driven analysis.

Respectfully submitted,
UNITED STATES TELECOM ASSOCIATION

By:



Robert Mayer
Kevin Rupy

607 14th Street, NW, Suite 400
Washington, D.C. 20005

November 14, 2011