From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 17th, 2010
Subject: Comments on "National Broadband Plan Recommendation
to Create a Cybersecurity Roadmap

Thank you for the opportunity to submit comments on the FCC's "National Broadband Plan Recommendation to Create a Cybersecurity Roadmap," PS Docket 10-146, GN Docket 09-51, released August 9th, 2010 [1]

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight all forms of abuse, such as phishing, botnets, fraud, spam, viruses and denial-of-service attacks. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, as well as from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (www.MAAWG.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and facilitation of collaboration.

Among other questions, your notice invited commenting parties to address the crucial issue of "What are the most vital cybersecurity vulnerabilities for communications networks or users?" From our perspective, the five most pressing cybersecurity issues for communication networks and users are as follows:

1. Spam, Phishing and Other Messaging Abuse

We believe the single most vital cybersecurity issue facing communication networks and users has been, and continues to be, messaging abuse, including both spam and phishing.

Spam and phishing are mainstays of the underground economy, facilitating and motivating much of the malicious behavior that takes place there. For example, spam is the customary "bearer service" for the delivery of phishing messages and consumers' PCs are routinely targeted by malware to create new "bots" (hidden automated email robots) that can be used to send spam.

The FCC already has commendable and effective anti-messaging abuse policies in place for wireless devices [2]; however ISPs in the United States and abroad continue to have substantial messaging abuse-related challenges, particularly in the wireline/broadband area. We recognize that messaging abuse in the wireline/broadband environment has traditionally been an FTC (rather than FCC) activity, but given the FTC's many responsibilities and its limited resources for enforcing CAN-SPAM, and keeping in mind the FCC's recently expanded role with respect to broadband, we think a collaborative interagency approach to dealing with the continued problems of spam and messaging abuse could be productive.

2) Unpatched Client-Side Software, Malware and Botnets

As mentioned previously, it is well known that the vast majority of the spam we see is sent by bots commonly created by malware successfully attacking unpatched PCs. SANS agrees with us that unpatched client-side software, malware and botnets (networks of affiliated bots) are important: their “Top Cyber Security Risks” report’s top priority is "Client-side software that remains unpatched." [3]

3) Vulnerable Internet-Facing Websites/Insecure Web Applications

Increasingly, as control of email improves, much spam is moving to the Web and malware is getting dropped on users from compromised websites rather than by email. We need to harden Web servers and the applications running on them so that problems on the Web do not result in the creation of newly compromised PCs, breaches of personally identifiable information, and other unacceptable outcomes.

Support for inclusion of this issue as a top cybersecurity concern can be seen in SANS listing "Internet-facing web sites that are vulnerable” as its number two priority [4]. We also note that the Department of Commerce explicitly called out “Web Site and Component Security” as one of only eight major focus areas for its recent request for comments relating to “Cybersecurity, Innovation and the Internet Economy” [5].

4) Distributed Denial of Service (DDoS) Attacks

Because the FCC has framed its inquiry in the context of the communications infrastructure, we cannot ignore the issue of distributed denial of service (DDoS) attacks. See, for example, Arbor's "Fifth Annual Infrastructure Security Survey," February 2010 [6].

As noted on the fourth slide of that talk, the largest anticipated threat for the next 12 months reported by survey respondents is "Link, Host or Service DDoS," as chosen by ~35% of all respondents. "Botnets" was the second most serious threat, accounting for 21%.

We do not need to look very far to see recent examples of how disruptive DDoS attacks can get. For example, consider the recent withering 50 gigabits-per-second attack conducted against DNS Made Easy [7].

5) Failures of Critical Network Infrastructure Chokepoints

Again, keeping in mind the FCC’s interest in communications infrastructure, we cannot ignore the risk of failures in critical network infrastructure chokepoints. This includes damage to physical facilities such as sub-oceanic cables and cable landing points, carrier hotels and major collocation facilities, among others. These outages can be due either to intentional vandalism, as was the case in Silicon Valley in April 2009 [8], or natural causes, as was the case for the APCN2 cable, severed by a typhoon in August of that year [9].

More attention needs to be paid to hardening or eliminating network infrastructure chokepoints if we are to maintain the sort of availability and reliability we all need. Obviously a focus on improved availability is consistent with the three classic information security goals of confidentiality/integrity/availability.

In conclusion, we believe these are the five key areas where the FCC should be focusing its cybersecurity efforts on behalf of communication networks and their users.

MAAWG would like to thank you for the opportunity to submit these comments for your consideration, and we would welcome the opportunity to offer further assistance to the Commission on its work in this important area. Please feel free to contact us if you have any questions, or if we can be of any further assistance.

Sincerely
/s/
Jerry Upton
Executive Director
Jerry.Upton@maawg.org

Notes:

[1] http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0809/DA-10-1354A1.pdf

[2] http://www.fcc.gov/cgb/consumerfacts/canspam.html

[3] http://www.sans.org/top-cyber-security-risks/summary.php

[4] ibid

[5] http://www.ntia.doc.gov/frnotices/2010/FR_CybersecurityNOI_07282010.pdf

[6] http://www.nanog.org/meetings/nanog48/presentations/Tuesday/Labovitz_SecSurvey_N48.pdf

[7] http://www.theregister.co.uk/2010/08/09/dns_service_monster_ddos/

[8] http://www.eweek.com/c/a/Messaging-and-Collaboration/Major-Phone-Internet-Outage-in-Silicon-Valley-752853/h(URL split due to length)

[9] http://www.zdnetasia.com/apcn2-cable-cut-cripples-connections-62056838.htm