**To:** National Institute of Standards and Technology, United States Department of Commerce

**From:** Messaging Anti-Abuse Working Group (MAAWG)

**Date:** November 3rd, 2011

**Subject:** Comments on "Models to Advance Voluntary Corporate Notification to Consumers Regarding the   
 Illicit Use of Computer Equipment by Botnets and Related Malware"

To whom it may concern:

Thank you for the opportunity to comment on the Departments of Commerce (DoC) and Homeland Security (DHS) "Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware," http://www.federalregister.gov/articles/2011/09/21/2011-24180/  
models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of#p-6 (hereafter "the RFI").

***I. Introduction***

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit, industry-led organization founded to fight online 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, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG ( http://www.maawg.org/ ) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards and the facilitation of global collaboration.

Our comments in this document generally follow the order in which topics were introduced in the RFI. In some cases, unless we've misunderstood the RFI author's intent, essentially the same question appears to have been asked multiple times. When we've notice that, we've generally will only responded once, referring the reader to our earlier response when the same (or an extremely similar question) is subsequently reasked.

We would also like to take this opportunity to remind the reader of MAAWG's earlier submission, dated July 29th, 2011, to the Department of Commerce Internet Policy Task Force's green paper on "Cybersecurity, Innovation and the Internet Economy," www.maawg.org/sites/maawg/files/news/MAAWG\_DoC\_Internet\_Task\_Force-2011-08.pdf

We would like to incorporate and reiterate the points that we expressed in that document here, and in the event there may be an actual or apparent conflict between the perspective expressed in this document, and the perspective expressed in the earlier document, the positions expressed in the preceding document should be considered definitive unless an express note disclaiming that earlier perspective is made herein.

***II. The "Background" Section of the RFI***

**1. Overall Goal of the Department of Commerce/Department of Homeland Security Initiative**

The RFI states:

*Through this Request for Information and any follow-on work, the two Departments aim to   
 reduce the harm that botnets inflict on the nation's computing environment.*

MAAWG strongly supports this overall goal, and commends the Departments for undertaking this important inquiry. Bots are a top priority for MAAWG, and we believe they should be a top cybersecurity priority for the   
DoC and DHS as well.

We may not always agree on all the precise details, but we definitely agree that working to reduce the prevalence and impact of botnets is critical to the security of the global Internet, and all its users.

**2. CSRIC's Best Practices for Botnet Protection and IETF Recommendations for Botnet Remediation**

In providing background information and context for the inquiry, the RFI mentions two pieces of prior work which MAAWG agrees are particularly noteworthy, and both of which MAAWG also strongly supports and endorses:  
  
— The work of the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 8, which produced two dozen best practices address botnet protection for end users and networks (see the   
RFI at footnote 9), and

— the IETF draft "Recommendation for the Remediation of Bots in ISP Networks," most recently  
http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-16 (expires March 24, 2012)

We would like to explicitly note and commend the hard work of all participants involved in that work, including the work and leadership of MAAWG-affiliated inidividuals. Notwithstanding these excellent prior efforts, obviously much work still remains to be done.

***III. The "Incentives and Voluntary Approaches" Section of the RFI***

**3. Potential "Safe Harbor" Provisions**

The RFI begins this section with the comment:  
  
 *To promote voluntary best practices in botnet detection, notification and mitigation, one   
 suggestion has been to provide companies that take action with certain types of liability   
 protection in order to foster greater marketplace certainty.*

ISP liability worries, to the extent they exist, are a reflection of the litigious society in which American ISPs exist. An ISP, acting in the capacity of a "good Samaritan," voluntarily undertaking to identify, notify and help a customer remediate infected systems, may all-too-often find themselves the target of customer ire, rather than customer appreciation:  
  
 — Users, not understanding the sometimes-proprietary technical approaches used to identify botnet infected  
 hosts, may view unexpected notifications about botnet infections as potentially privacy invasive or   
 intrusive ("How do *you* know that my computer is infected? Have you been spying on me? I'm going to sue  
 you!")

— Notifications, unless persistent or done in a way which is impossible to ignore, may be disregarded;

if done in an impossible-to-ignore way, users may resent those contacts ("Quit bugging me or I'm going to  
 call my attorney!")

— Efforts to help users attempt to remove malware from their system may subject an ISP intervener to   
 putative liability for any subsequent issues that system may experience, whether related to the malware  
 infection, the ISP's efforts to help remove that malware, or some wholly unrelated cause ("My system has

been screwed up ever since you tried to remove the malware you claim was on it, and there's *still*  
 something wrong with it! Thanks for *nothing* -- I'll see *you* in court!")

Providing ISPs with limited immunity from legal liability for their voluntary efforts to combat bots has the potential to at least remove one potential obstacle to ISP efforts in that area -- litigation exposure -- and as such, it would be welcomed, *provided* that it does not inadvertently or unintentionally serve to provide *disincentives* for ISP intervention.

An example of liability protection that would be *counterproductive*, disincenting ISP action against bots, might be offering ISPs the option of obtaining complete "common-carrier"-like immunity from liability, whereby they literally just provide connectivity and have no responsibility (or even ability) to do anything beyond simply providing transport. MAAWG would oppose any such effort as ultimately counterproductive and contrary to the best interests of its members and the Internet as a whole. ISPs *must* remain involved and engaged in the war against bots.

Ultimately, however, even if a statute can protect an ISP from litigation, no statute can immunize an ISP from the potential economic impact of disgruntled customers "voting with their pocketbook." Even if a customer is prevented from suing an ISP, most customers will continue to have the option of moving to another ISP if they are sufficiently dissatisfied with how their current ISP works with them, whether that's in conjunction with fighting an infection or some unrelated issue.

Thus, even if an ISP is offered limited immunity from liability by statute, many ISPs may nonetheless be inclined toward employing a "light touch" when it comes to undertaking customer botnet identification, notification, and remediation, unless ALL market participants are required to meet a common standard.

Immunization from liability also doesn't address a related basic but critical issue: ***who will pay?*** While limiting liability removes one ***potential*** financial obstacle (the risk of litigation), ISPs are still faced with the ***actual*** operational costs associated with providing identification, notification and remediation services. On balance, the value of the proposed limits on liability may be small for most ISPs relative to those concrete and ongoing operational costs.

Thus, immunization from liability might best be viewed as helpful, or enabling, but liability-related concerns are not the only obstacle that may deter some ISPs from proceeding with botnet identification, notification, and remediation tasks.

**4. The "Centralized Consumer Resource Center" Concept**

The RFI describes this notion as follows:  
  
 *Another suggestion is to encourage ISPs to send consumer support queries to a centralized consumer  
 resource center that could be supported by a wide number of players. Such a resource center could  
 reduce the burden on corporate customer support centers by pooling resources. The center could aid   
 consumers by, for example, providing certain no-cost means of support, as well as information on   
 other means for expedited support. This center could also be used to facilitate information sharing   
 and research that could lead to better botnet detection. Moreover, as a “condition of sponsorship”   
 private sector entities could be required to adopt an agreed upon set of practices.*

The RFI then goes on to describe several potential models for that center (wholly private, mixed private/public, wholly public).

In thinking about this concept, MAAWG has concerns about the extent to which this concept will be practical/scalable. Please remember:

— Many online technical self-help resources for botted system owners ***already*** exist. Why would creating *yet   
 another* such resource succeed if existing resources haven't?

— Most botted systems are owned by average men and women, not technical enthusiasts. Extensive "hand holding"

will likely be needed to help these users, not just a few quick tips. To get some idea of the magnitude of what   
 might be required, consider the following scenario:  
  
 -- Assume each botted user requires an hour's worth of a technician's time (note that that's a very conservative   
 (low) estimate, and can easily be a factor of 2X or more higher),

-- While the RFI quotes a figure of 4,000,000 new botted hosts per month, let's assume that there are only  
 on average 100,000 new U.S.-origin botted hosts per week that might contact the proposed center

-- Simplifying for the sake of this model, assume that all technicians can be efficiently scheduled (in reality, users  
 would likely seek help from the center in "lumpy" ways, "mobbing" technicians during some intervals, such as   
 after new malware is released, and leaving them largely idle during other hard-to-predict periods)  
  
 -- We assume that the technicians work forty hour work weeks, and there's no lost time due to meetings, training,  
 vacation time, or other normal non-productive periods  
  
 That implies that the center would need a minimum of (100,000/40)=2,500 technicians, year in and year out.  
 If the center hires moderately skilled employees, we might expect a fully loaded salary cost of $60,000 per  
 technician, including direct salary, benefits, and required equipment (computer, network connectivity,  
 telephone access, office furniture, software, documentation, etc.).

$60,000\*2,500=$150,000,000/year. That's a daunting budget for these budget-constrained times.

— Anyone who has worked in technical support can tell you that it is very inefficient to walk users through a   
 complex (multi-step) technical process over the phone. If the proposed model is one where all contact is via  
 telephone, fax, or email, our initial estimate of an hour per user is truly wildly optimistic. If the proposed  
 model envisions users bringing their systems in for help, or technicians making house calls, the center will   
 need to be broadly distributed, the cyber equivalent of local extension agents trained to diagnose and recommend   
 treatments for crab grass and other agricultural or horticultural maladies. We don't believe that that's the model   
 that's envisioned, however. We believe that the hope is that users will be able to get help online, and then   
 self-remediate once they've received some initial tips, even if in fact that's impractical.

— Most users will not have even the basic software tools they might need to remediate an infected system, and   
 the presence of malware may make it difficult or impossible for them to download the tools they'd need, either   
 because malware is actively blocking access to known remediation resources, or because their ISP has disabled   
 their access to the Internet once malware was detected on their system.

— Even if users had some of the more commonly suggested tools for tackling an infection, running an antivirus   
 program, even with completely up-to-date antivirus definitions, may not be able to find and remove all the   
 malware that's infecting their system. That's why most computer security experts recommend that users "nuke   
 and pave" (format and reinstall) an infected system, rather than trying to remove malware without rebuilding.  
 That strategy naturally presumes the existence of clean and trustworthy recent backups of user files, backups   
 which may not in fact exist.

— Even if a system can be disinfected, or rebuilt from scratch with clean backups, if the system isn't patched and  
 otherwise hardened, it may only be a matter of time before that system gets re-infected. Patching and hardening  
 a system requires a careful balancing of user requirements against user risks, a balance that varies from user to   
 user, and something that may not be able to be standardized in a one-size-fits readily-automated way.

### IV. The "General Questions on Practices To Help Prevent and Mitigate Botnet Infections" Section

***(1) What existing practices are most effective in helping to identify and mitigate botnet infections? Where have these practices been effective? Please provide specific details as to why or why not.***

Specific techniques used by ISPs and security vendors to identify and mitigate botnet infections are seldom publicly discussed in detail out of a desire to avoid inadvertently helping bot herders avoid detection, and out of a desire to protect sources and methods. For those reasons, and mindful of the fact that this response will be publicly available, we will limit our response to the first part of this question to the following basic points:

(a) ***We assume that we're discussing a network that is "well instrumented,"*** e.g., one that at least routinely collects Netflow data or the equivalent for traffic that passes over it. Note that it may not always be easy to extensively instrument one's network, particularly if:  
  
— The network is operating at 40Gbps or 100Gbps, speeds at which monitoring may be technically   
 challenging, or  
  
— The as-deployed network architecture requires instrumentation at a large number of discrete  
 locations, rather than a relatively small number of core nodes, or  
  
— The network carries IPv6 or other advanced protocols, protocols which may not be readily

measurable on some networks.  
  
(b) ***The easiest way to identify bots in bulk is by monitoring network traffic for the bots emissions.*** For example, if a botnet is used to send spam, the spam emitted by that host is the tell-tale indicator that that host is botted. That spamming may be directly noticed by Netflow processing software, or the spamming may be noticed as a result of other factors (potentially including things as simple as complaints from other sites, or distinctive patterns associated with the bots use of DNS).

Not all types of bot emissions may be directly attributable to their actual source. For example, consider a DDoS bot emitting spoofed UDP traffic: once that traffic exits the source network, it may be difficult or impossible to directly attribute its true origin. If more networks employed BCP38 filtering of spoofed traffic, this would be less of a problem, but as noted by the MIT Spoofer project (http://spoofer.csail.mit.edu/index.php), over 20% of all autonomous systems continue to allow the emission of spoofed UDP traffic by their customers. That is a concrete example of something that an ISP voluntary code of conduct might explicitly seek to change.

***(c) Once a botted host has been identified from its emissions, one approach to identifying additional hosts that are also botted, even if they aren't yet emitting spam or other problematic traffic, is to "look upstream."*** That is, bots tend to be controlled via commands issued from command and control ("C&C") hosts. Botted hosts "check in" with their C&C hosts, and then subsequently receive instructions from that C&C. Those instructions might direct a bot to update or extend itself by downloading new software, or it might tell the bot to send spam, or DDoS a particular targeted site. Obviously, once you know a C&C exists, communication between that C&C and one of your users' systems is a sign that something is likely seriously amiss.

With respect to the questions, "Where have these practices been effective? Please provide specific details as to why or why not," again, recognizing that this is a sensitive question, we will limit our remarks to the following points:

(d) Networks have to ***be interested in identifying, notifying and mitigating botted customer hosts.*** If network operators aren't interested in doing so, botnet identification, notification and mitigation won't occur. Distinguish three main reasons for a potential lack of interest:  
  
— Dealing with infected customer is potentially expensive, and if not required, represents an  
 avoidable expenditure that will otherwise potentially reduce the profitability of the ISP.

— While the tradition among early sites on the Internet was that each site had an obligation to be a   
 "good neighbor," taking care of any abuse originating from its facilities, later Internet entrants   
 often brought with them a different perspective, e.g., that they were a quasi-common carrier, and  
 that their responsibility was simply to provide connectivity to users on a non-discriminatory   
 basis, with no obligation (or even ability) to "interfere" with how that connectivity got used. If you  
 have the perspective of those later entrants, policing the Internet was the responsibility of, well,  
 the police, even if law enforcement had no mandate or ability to operate effectively in that space.

— Other companies have been known to ***intentionally*** turn a "blind eye" to what happens on their   
 networks, receiving a premium price from malicious customers for offering "bullet proof" service.

(e) Network based bot detection solutions require a ***well-instrumented network***, as was discussed previously. If a network isn't built and configured in a way that allows the network operator to monitor its own facilities, it will be "driving with blinders on," and that network operator will have a hard(er) time identifying botnets that have established themselves among their customers, or confirming complaints that they may receive.

(f) Network operators need the ability to ***communicate effectively with their customers****,* most typically via email. That ability may not always exist.   
  
While many operators may routinely provide their customers with email accounts, customers may not use them, perhaps preferring an email account obtained at work or school, or a free account obtained from Gmail, Hotmail, Yahoo or some other provider. The network operator may have no idea what their customer's preferred email account -- the one they actually use/read -- might be.

Even if the network operator does know its user's preferred email address, customers may be wary of trusting or relying on "warnings" received by email since they will often have routinely received wave upon wave of phishing messages, and may not be able to distinguish a real warning from a fake one.  
  
Alternative communication channels, such as calling the customer on the phone, or sending the customer a written letter by US Mail, may be too expensive, and may be routinely ignored or disregarded as a likely marketing contact by their ISP.

Ultimately, the contacts that are hardest to ignore and most credible are probably those that may be provided as part of a captive portal strategy. That is, when a customer is identified as infected, they may get put into a special VLAN that limits the sites they can access until they've cleaned up their system.

As part of that process, users may receive advisory communications directly in their web browser, in lieu of (or in addition to) their normal home page or some site they'd expected to visit. By demonstrating control over the user's web experience, such messages are both hard to ignore, and demonstrably credible.

(g) ***Network operators also need the ability to communicate and share cybersecurity data with each other.*** For example, if an ISP is seeing incoming spam from another ISP, the ISP that's receiving that spam should ideally be able to share evidence of that abuse with the originating ISP. Attempts to create data sharing arrangements of that sort may be challenged as a result of technical and policy-related concerns, including:  
  
— A lack of usable points of contact for some providers (RFC2142 role accounts may not exist, or if   
 they exist, they may not be read and acted upon)

— Some ISPs may apply consumer grade anti-malware and anti-spam filtering to abuse reporting  
 addresses, thereby making it hard to report malware and spam with necessary evidence  
  
— Different providers may employ or prefer different reporting formats (for example, should reports   
 be exchanged in RFC5965 "ARF" format, or is some other format needed?)

— When abuse reports are shared, are they shared in an un-redacted format, or do privacy   
 considerations mandate redaction of potential customer-identifying data?

— Should all abuse reports be forwarded, or just a representative sampling (such as 1-in-10 or  
 1-in-100)? If too many reports are forwarded, it may have the effect of DDoS'ing the abuse   
 reporting address; if too few reports are forwarded, some particular abuse incidents may end up

"slipping through the cracks."

Some ISPs have successfully tackled these issues, and Spamhaus lists 15 providers of such "feedback loops" at http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#119  
  
Encouraging ISPs to offer feedback loops, to have monitored abuse reporting addresses, and to avoid over-filtering those abuse reporting addresses, are nice examples of potential elements of a voluntary code of conduct for ISPs.

(h) ***Sometimes simply identifying an actual botted host may be difficult.*** This is particularly true for sites that make extensive use of NAT with PAT, sharing a single public IP addresses with scores or even hundreds of internal hosts. Which "needle in that haystack" is actually infected? As IPv4 exhaustion plays out, and use of IPv6 or carrier grade NAT becomes common, this issue will become only more common.

***(2) What preventative measures are most effective in stopping botnet infections before they happen? Where have these practices been effective? Please provide specific details as to why or why not.***

Many practices are effective, or at least potentially effective, in stopping botnet infections before they occur. Some of those practices include:

(a) ***Bots are strongly associated with Microsoft Windows.*** Use of an operating system other than Microsoft Windows (such as Apple Mac OS X, or Linux), will reduce your risk of having your system get botted (although naturally it is impossible to predict future directions that botnets might take).

That said, consumers continue to find Windows to be an attractive operating system, with a wide variety of available applications, and one that's routinely available on systems that may be less expensive than some alternatives. In the enterprise space, Windows also has excellent manageability for centrally managed IT shops, which may be one reason why properly administered enterprise Windows deployments are seldom seen broadly botted.

(b) Regardless of what operating system gets run, it is critical that system's be kept ***patched up to date***, including the operating system itself, as well as all applications (such as office suites and browsers that may be installed) and also including helper applications that may be installed (such as Adobe Acrobat Reader, Flash, Java and QuickTime). Secunia PSI/CSI/OSI may be tremendously helpful in identifying installed applications that are in need of patches.

(c) Systems often come with many unneeded services or protocols enabled by default. This increases the system's potential "attack surface." Thus, an important step is to ***disable any unneeded services or protocols***. Put tangibly, if a user self-tests their system with a port scanning utility such as GRC's ShieldsUp (https://www.grc.com/x/ne.dll?bh0bkyd2), few if any ports should show as open.

(d) Hardware or software ***firewalls*** have historically been another staple "common sense" recommendation, and were potentially helpful in deflecting historic "scan and sploit" remote attacks.

Unfortunately, traditional firewalls are unable to protect systems against malware that's dropped when a user unknowingly visit a tainted web page. Firewalls may also limit throughput, interfere with H.323 video conferencing or the use of native IPv6, and serve as a potential stateful chokepoint for denial of service attacks. Their value is thus something of a mixed bag at this point, even though many users continue to rely on them, at least at home. (And laptop or mobile device users may have relatively few options when travelling and connecting via third party wireless access points, except for on-device software firewalls)

(e) ***Antivirus products*** routinely get mentioned as an important part of every user's strategy for avoiding malware infections, however, increasingly, the pace of malware production and release may be outstripping the ability of some antivirus companies to keep up. As a result, even users who are running a leading commercial antivirus product with up-to-the-minute antivirus definitions may still be vulnerable to infection by malware.

(f) Users need to use ***strong (long/complex) passwords*** for their systems and online accounts, and need to strive to avoid allowing those passwords to be sniffed or phished. When supported, two factor authentication (such as use of a hardware cryptographic fob in addition to just a password), or two channel authentication (such as use of a code sent to a user's smart phone in addition to just a password), can dramatically reduce the ability of bots to take over user accounts.

(g) The principle of "least privilege" means that if you don't need particular privileges, you should avoid using them when performing routine tasks. In this context, that means that users can minimize the potential impact of any malware they encounter by ***not running as a privileged user*** ("admin," "root," or the equivalent) ***except when necessary*** for software installation or other maintenance.

(h) Javascript is pivotal to many highly popular interactive sites. However, Javascript can also serve as a common path for dropping malware on user systems. Some users have thus taken to either ***blocking Javascript*** outright, even if that means forgoing some hugely popular web sites, or using a tool such as NoScript for Firefox to block Javascript when an untrusted site attempts to use it for potentially malicious purposes.

(i) Many useful sites are underwritten by revenue from online advertising. However, recognizing that advertising is not essential to most users, and that malware can be unintentionally delivered via advertising sites, some users, uninterested in seeing ads on the web pages they visit, use tools such as AdBlock Plus for Firefox to ***block content from advertising sites***. In doing so, those users reduce the likelihood that they will be a victim of "malvertising," malicious software delivered via advertising sites.

(j) ***Avoid using peer-to-peer applications, or trusting files downloaded from P2P sites.***

(k) Another approach is for ***ISPs to deny malware authors access to reliable DNS*** (domain name service). Currently, most sites faithfully resolve malicious domain names just as they would the domain name of legitimate sites. Paul Vixie of the ISC, author and proponent of RPZ ("Response Policy Zones"), urges ISPs and users to deny miscreants the ability to rely on DNS. Specifically, if ISPs blackhole (filter) known malicious DNS resource records, cyber criminals will no longer be able to use DNS to resolve malware dropping sites, command and control hosts, phishing sites, etc.

All those approaches, and many, many, more, have been tried by users and sites in an effort to pre-emptively block botnets. When employed conscientiously, they typically result in a material reduction in hosts being botted. When they are employed less conscientiously, less protection is delivered and more compromised hosts are observed.

A nice starting point for users interested in steps they can take to harden their systems can be found at the National Security Agency Central Security Service's Security Configuration Guide site, see  
http://www.nsa.gov/ia/guidance/security\_configuration\_guides/operating\_systems.shtml

***(3) Are there benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise? If so, why and how? If not, why not?***

To answer this question we must consider what happens if a voluntary code of conduct is ***not*** developed and standardized.

If such a code of conduct is not developed and standardized, one potential result might be mandatory federal regulation. As the lesser of two evils, most ISPs would agree that a voluntary code of conduct would be preferable to mandatory federal regulation, particularly if those regulations represented an unfunded mandate, or mandatory federal regulations had no way of keeping up with the rapidly evolving threats that ISPs constantly face.

Arguing in the alternative, given that we've seen consistent grid lock at the federal level when it comes to passing cyber security legislation, we must also recognize that the possibility exists that mandatory federal cybersecurity regulations are simply too contentious to get passed into law at this time. In such a case, imperfect though a voluntary code of conduct might be, it might be the best that the community can do when it comes to clearly defining minimum community expectations for cyber security.

In either case, we must recognize that a voluntary code of conduct will likely be embraced most strongly by those who already proactively take all feasible steps to deal with botted customers. Those who are ambivalent, or who actively conspire with cyber criminals, are unlikely to change their behavior as a result of the creation of a voluntary code of conduct, absent economic incentives.

We also need to recognize that some ISPs may claim that they intend to follow a voluntary code of conduct, while failing to actually do so. Some thought should be given to how agencies might deal with entities that claim to adhere to a voluntary code of conduct, while flouting the terms of that code in practice.

***(4) Please identify existing practices that could be implemented more broadly to help prevent and mitigate botnet infections.***

Please see our responses to questions (1) and (2), above.

***(5) What existing mechanisms could be effective in sharing information about botnets that would help prevent, detect, and mitigate botnet infections?***

Distinguish two types of "information sharing about botnets:"  
  
— ***General*** best common practices (BCPs) for preventing, detecting and mitigating botnet infections, and  
  
— ***Specific*** operational details about observed botted hosts, botnet command and control hosts and their name   
 servers, sources of botnet infections, and related specific data-driven "actionable intelligence."

MAAWG and other industry organizations routinely share "BCP" information of the first sort in an effort to help its members and third parties to cope with the problems that botnets can cause.

Specific data-driven actionable intelligence about botnets is also broadly shared within the community.

We've already mentioned (see IV. (1) (g), above) that some ISPs have created feedback loops designed to share information about botted hosts that are emitting spam. That is a fine example of sharing data-drive actionable intelligence about botted hosts.

Another example of data-driven actionable intelligence can be seen in various DNS-based blocklists, such as those offered by Spamhaus, or the SURBL. If an ISP has IPs or customer domains on those blocklists, they've likely got botted customers.

Data-driven operational intelligence can also form the core of a proprietary for-fee security service offering from a commercial entity or entities, or may serve as the entire *raison d'être* for the purchase of some types of network security appliances.

In other cases, actionable intelligence about botnets may be shared at no cost, but only on a need-to-know basis   
(the goal in that case will typically be protecting the sources and methods used to develop that operational intelligence, or avoiding retribution from disgruntled bot herders).

***(6) What new and existing data can ISPs and other network defense players share to improve botnet mitigation and situational awareness? What are the roadblocks to sharing this data?***

ISPs and other community participants can share:  
  
(a) ***IP addresses*** (with timestamps) of botted hosts observed to be spamming or otherwise misbehaving (see  
 for example http://www.spamcop.net/w3m?action=inprogress )

(b) ***Spamvertised domain names*** (or other points of contact to which replies are being directed, such as phone  
 numbers or throw away email addresses); see for example   
 http://www.spamcop.net/w3m?action=inprogress;type=www

(c) ***Botnet command and control host information*** (see http://mtc.sri.com/live\_data/cc\_servers/ )

(d) ***Name servers*** used by the above

(e) Information about ISPs that may be routing botnet-related infrastructure (e.g., ***ASNs*** that are routing   
 botnet-related netblocks)

(f) Attribution (owner/user) information associated with botnet-related assets, including ***IP whois and domain   
 whois*** information, and any shell companies or fake identities used to purchase domains names, hosting services,   
 or other infrastructure used by bot herders or bot users.

(g) Details of affiliate programs associated with bot-spammed email (e.g., ***affiliate codes*** associated with spam)

(h) ***Malware samples (or hashes)*** associated with botnet infections; analyses/reverse engineering writeups   
 associated with such malware

***(7) Upon discovering that a consumer's computer or device is likely infected by a botnet, should an ISP   
or other private entity be encouraged to contact the consumer to offer online support services for the prevention and mitigation of botnets? If so, how could support services be made available? If not, why not?***

Yes, we believe the consumer ***should be notified*** whenever possible, however the details of the support services (if any) that may be appropriate beyond that will vary depending on the circumstances of the observed bot.

As previously discussed, in many cases botted hosts are not able to be readily disinfected. That is, it is ***not*** just a matter of saying, "Download the antivirus product we've provide for your use, and run that software to clean up your system," any more than a user should be expected to self-treat a case of tuberculosis or cancer.

It would be terrific if there was a "magic bullet" that could cure all malware, or all human diseases, but we've yet to discover that sort of magic potion.

In the case of a malware-infected system, many things can prevent a self-help strategy:  
  
(a) ***The malware may interfere*** with the user downloading or executing the recommended antivirus product,

(b) If the user is able to download and run the antivirus product, it may not ***detect*** the malware that's infecting the host,

(c) if it does detect the malware, it may not be able to safely (or completely) ***remove*** it,

(c) If the user does succeed in removing the malware, they may still be infected with ***other malware***,

(d) the malware they just removed may quickly be ***reinstalled*** unless their system's underlying vulnerabilities are corrected, too.

Bottom line, online self-remediation is simply ***not*** sufficient to cure most botted hosts.

***(8) What should customer support in this context look like (e.g., web information, web chat, telephone support, remote access assistance, sending a technician, etc.) and why?***

Most commercial malware remediation services ("rent a technical support person"-type outfits) offer three basic models:  
  
— Help at the user's site (they make a "house call" to your home or business, typically the most expensive option)  
  
— Help at the service provider's location (you bring your system to the service provider, the least convenient option,  
 from a user's point of view, at least for desktop systems)  
  
— They work with you online (this option presumes that your ISP has not cut off your connection, and that malware  
 isn't actively interfering with remediation efforts); this is typically the least expensive option.

Most users predictably prefer the cheapest and easiest option for their particular circumstances.

For a rational user who's paying for remediation services out of pocket, the upper bound on what they should be willing to pay for remediation services should be:  
  
 The cost of a new system +

The cost of transferring critical applications and user files from the old system or backups –  
 The expected salvage (resale) value of their old system =   
  
 The rational ceiling on potential remediation expenditures

Users may also perceive an intangible value to buying a new system that may be faster or more reliable or have more features than the old system that it's replacing.

Today's reality, however, is that perfectly serviceable new Windows laptops are available for $500 or less, and new Windows desktops are less expensive still. This means that if a user has a severely infected system, particularly one that is now multiple years old, they may be better off replacing that infected system rather than spending hundreds of dollars either attempting to clean it, or executing a nuke-and-pave (format and reinstall) strategy.

But the preceding is all thinking about this from an end-user's point of view.

From the point of view of an ISP, the form that customer support should take depends on:  
  
— the scale at which you need to provide it (one user? a hundred users? ten thousand users?)

— your goals in providing that support,

— the technical expertise of the customer, and

— the specific characteristics of the malware infecting the systems.

If you're a small local ISP and only need to help a handful of botted customers a day, having an otherwise-not-busy technician informally make a house call may provide the best customer experience.

However, if you have thousands or tens of thousands of customers who need help a day, and those customers are spread across a broad geographic region, it may not be practicable for an ISP to dispatch a technician to fix their infections on site (or more accurately, it would be prohibitively expensive for them to do so).

Conservatively, assume that even the briefest of house calls costs a minimum of $75, considering staff costs such as salary and benefits, the cost of providing a vehicle and fuel, hardware and software tools for use by the staff person, insurance against errors and omissions, etc. Given today's highly competitive marketplace and slim realized margins, the expense associated with a single house call of that sort would likely wipe out any profit from that customer for months if not years to come.

Passive delivery of remediation information to consumers, e.g., via web pages, presumes an availability of tools and expertise that will only rarely be present. Without having those tools and specialized expertise, users will likely be overwhelmed attempting to self-remediate, and may actually make their circumstances worse (e.g., users can easily accidentally "brick" their system (render it unusable) while attempting to edit the Windows Registry).

Synchronous support via the telephone often takes a long time, as users need to locate and relay what they see on their screen, particularly in the case of non-technical users, or users who may be anxious over the possibility that they're going to "break something."

Attempting to short circuit that process by installing a remote access client, allowing the technician to temporarily take control of the user's system for diagnosis and remediation purposes, raises questions of user privacy and trust: in most cases, remote access clients give the remote technician complete access to the user's system, and all the potentially sensitive information that may be stored on it (personal email; documents and photographs; saved passwords; past tax returns; etc.). How is the user to know that their sensitive information, and their irreplaceable content, won't be leaked or accidentally lost? How is the user to know that the remote access capability has been disabled or de-installed, when it is no longer needed?

***(9) Describe scalable measures parties have taken against botnets. Which scalable measures have the most impact in combating botnets? What evidence is available or necessary to measure the impact against botnets? What are the challenges of undertaking such measures?***

We might best begin by considering what makes a potential anti-bot measure scale ***poorly***:  
  
— A ***human being is involved*** somewhere along the line (e.g., the user needs to do something, or an ISP customer  
 service technician needs to do something, etc.). You need to be able to leverage automation rather than rely on   
 slow and error-prone human intervention  
  
— A systematic understanding of the underlying phenomena is lacking, so structural weaknesses haven't been  
 identified for eventual exploitation (as an example, imagine that botnets are leveraging fast flux hosts are   
 defenders attempt to identify and take down participating hosts one at a time, rather than going after the  
 fast flux name servers or domain name registration, instead).

That is, poor scalability is often associated with a solution needs to be custom crafted for each case; scalability   
 suffers if there is ***no general-form solution*** that's broadly applicable.

— State needs to be ***maintained*** and "remembered" somewhere (access control lists in a firewall, router or other   
 network appliance; whitelists or blacklists of unwanted IP addresses or unwanted domain names; etc.)  
  
— State needs to be ***replicated and updated*** at many points, rather than being maintained at a centralized   
 location (how will you replicate and distribute that state to all the points that need a current copy of it?)  
  
— State isn't able to be ***cached***, so that the same query (and the same answer) might get asked and answered   
 repeatedly.  
  
— There is no strategy for "garbage collection" or ***cleaning saved state*** information that's no longer timely, thereby   
 resulting in accumulated state becoming diluted by irrelevant legacy information that really should have been  
 purged.  
  
— The strategy has a ***tangible cost*** (e.g., if I need to mail a CD to each infected user, that scales badly because of  
 the costs of creating and delivering those CDs).

Given those considerations, one can quickly see why truly scalable anti-botnet measures are usually either:  
  
— ***Network-based solutions*** (such as DNS-based blocklists); for example, Spamhaus currently protects   
 1,438,371,000 user mailboxes as of October 18th, 2011 (http://www.spamhaus.org/organization/index.lasso), or  
  
— ***Automated tools*** (such as Microsoft's Malicious Software Removal Tool, which runs each month as part of   
 Microsoft Update). Microsoft notes that the MSRT was downloaded and executed 3.2 billion times in the first  
 half of 2010 alone. (Microsoft Security Intelligence Report, Volume 10, January-December 2010, PDF page 72)

A concrete example of a **less**-scalable anti-botnet measure is the FBI's Coreflood Botnet takedown (see http://www.fbi.gov/news/stories/2011/april/botnet\_041411 ). While that effort was and is appreciated, and had a material affect on botnets, it required an awful lot of hard work by federal agents. If you are not familiar with that takedown, see, for example:

— "FBI vs. Coreflood botnet: round one goes to the Feds,"   
 http://arstechnica.com/tech-policy/news/2011/04/fbi-vs-coreflood-botnet-round-one-goes-to-the-feds.ars and   
  
— "FBI Begins Disinfecting Coreflood from User PCs,"   
 http://securitywatch.eweek.com/botnets/fbi\_begins\_disinfecting\_coreflood\_from\_user\_pcs.html

Why was that takedown less scalable?

— Extensive legal pleadings were required.  
  
— An attempt was made to allow users to "opt out" of having Coreflood removed (an option that few if any would   
 knowingly exercise), and to explicitly solicit user consent to clean the infection from their system.

— Anti-bot measures were only applied to infected systems located within the United States.  
  
— Ultimately many instances of Coreflood were deleted by the MSRT rather than by the direct actions of the FBI.

When it comes to measuring the effectiveness of those sorts of approaches, metrics are available.

For example, consider the Composite Block List (the "CBL", see http://cbl.abuseat.org/ ), the botnet-focused component of the Spamhaus blocklist. The CBL website offers a variety of metrics, including:  
  
— the distribution of botted hosts per domain, per country, per ASN, etc.

— a breakdown showing the botnets that it is routinely seeing

— a pointer to a comparison of various blacklists, see http://www.sdsc.edu/~jeff/spam/cbc.html

— and many other fascinating statistics.

Microsoft routinely shares information about the impact of their Malicious Software Removal Tool as part of their periodic Security Intelligence Report (SIR), see http://www.microsoft.com/security/sir/default.aspx (note: both a   
brief summary and a far more detailed report are provided at that site; be sure to see the detailed report for detailed MSRT-derived metrics)

***V. The "Effective Practices for Identifying Botnets" Section***

***(10) When identifying botnets, how can those engaged in voluntary efforts use methods, processes and tools that maintain the privacy of consumers' personally identifiable information?***

We assume that the departments issuing this RFI did not use the term "personally identifiable information" casually, but rather as a term of art. We therefore need to begin by defining what we consider to be "personally identifiable information."

Sensitive categories of PII are normally considered to include things such as:

— credit card or debit card numbers (particularly if the card holder's name, billing address, card expiration date and   
 CVV codes are included)  
  
— government assigned identifiers (such as SSNs, drivers license numbers, passport numbers, etc.)

— health-related information (e.g., medical records covered by HIPAA)

— financially-related information (e.g., bank records and other information covered by GLBA)

— educational records (e.g., FERPA-covered data)

— biometric or genetic data about a person, etc.

The sensitivity of those sorts of information increases when combined with other data, such as the user's name, or other user attributes such as their date of birth, likeness, height/weight/hair color and eye color, gender, race, marital status, disability status, veterans status, home address, telephone number, preferred email address, etc.

**Most sorts of sensitive PII are not routinely seen when exchanging information on botnets** -- or at least not in conjunction with consumers or other innocent third parties (a fundamental part of anti-botnet work does often involve accumulating details about known or suspected bot operators or supporting organizations, including affirmative efforts at preventing those cyber criminals from remaining anonymous and unattributable; by way of example, see the Spamhaus Register of Known Spam Operations (http://www.spamhaus.org/rokso/).

One potential exception may be user IP addresses. Some jurisdictions may hold that an IP address is potentially PII, while other jurisdictions have determined that it is not.

In fact, one of the reasons why ISPs are often viewed as playing a pivotal role in the fight against botnets is that average users enjoy a high degree of *de facto* anonymity online, unless they engage in activities that undercut that status.

For example, most users, when connecting to their ISP, will automatically receive a dynamic IP address. They will then use that address while working online. After a period of time (which varies from ISP to ISP, and can be a matter of mere minutes or multiple days or longer), the "lease" for that IP address will either be renewed or relinquished. The next time that customer connects, they will commonly receive a different IP address. (That's why the addresses are known as "dynamic," rather than "static").

While the user's ISP ***can*** normally map network activity associated with an IP address at a given point in time to a customer, only authorized employees of the ISP, with privileged access to the necessary network logs and business records, will normally be able to do so.

***External parties*** will generally NOT be able to do that sort of IP to name mapping, although there are exceptions.

As an example of a time when a third party can potentially map an individual's identity to their IP address, imagine that the user has logged in to a web site, and suppose that that account has been tied to their actual identity, perhaps as a result of the user making a purchase there with a credit card. Once that happens, the web site operator then has the ability to map that logged-in user's actual identity to their IP address, at least until such time as the user gets a new IP address (and even then, if the user remains logged in or cookies are being used, the web site may be able to continue to know the user's identity even as the user moves from one IP address to another)

Bottom line, consumer personally identifiable information is typically ***not*** at risk as a result of botnet identification-related efforts.

***(11) How can organizations best avoid “false positives” in the detection of botnets (i.e., detection of behavior that seems to be a botnet or malware-related, but is not)?***

False positives are rare when sound behavioral approaches are used to locally identify bots based on network traffic

(since normal customer network traffic doesn't look anything like the sort of network traffic emitted from a botted host).

That said, it is possible to conceive of some situations when false positives are a possibility, particularly in conjunction with external botnet notifications. For example:

— We must acknowledge the possibility of malicious and unfounded botnet related reports, perhaps made in an attempt to "punish" security researchers or others who are interfering with the conduct of online cyber crime. These reports are easily discredited by the ISP if internal netflow data is available, and the externally reported incident(s) cannot be corroborated.

— Sometimes there may be accidental confusion over time zones when bot detections are made, or clocks may not be well anchored to trustworthy NTP sources.

When that happens, and a dynamic address is involved, the mapping of an IP address to a user may go awry, pointing to an innocent user rather than an actually botted one. (Remember that a dynamic address may be used by one user at a given point in time, and then by some other user shortly thereafter -- distinguishing the two users requires accurate time stamps). Careful attention to time zone issues, attention to NTP synchronization, and work to confirm external reports using internal netflow data can mitigate these potential false positives.

— BGP route injection is another approach which may potentially obfuscate the true source of bot traffic. That is, if an abuser with a complicit ISP announces a more specific route for an already-in-use netblock, and then spams (or engages in other undesirable behavior) from that hijacked address space, the actual authorized user of that address space might end up getting "blamed" for that abuse even though that abusive network traffic may never have been anywhere near the actual authorized user's network. (For a discussion of this, see "Route Injection and Spam,"  
http://pages.uoregon.edu/joe/maawg8/maawg8.pdf ). Careful monitoring of wide area BGP routing data, and verification of external abuse reports against internal netflow data, can largely mitigate this risk.

— A malware researcher might intentionally download botnet-creating malware in a controlled way for analysis purposes. If network monitoring equipment doesn't know that this is intentional behavior by a security researcher, and not an accidental infection happening to an average user, it may flag that researcher's activity as a possible new bot infection.

— Primitive (and not-recommended) "botnet detection" heuristics may do things such as mistakenly flag any user connection to an IRC (Internet Relay Chat) server as a potential botnet command and control connection. While IRC is an admittedly popular botnet command and control technology, IRC can be, and is, used for legitimate purposes by hundreds of thousands of users worldwide every day.

— Naive reporters may not understand that UDP traffic, unlike TCP traffic, can be spoofed if the emitting network doesn't follow BCP38-recommended filtering practices. Thus, from time to time, you may encounter reports complaining about spoofed UDP traffic that "you" emitted.

— Non-technical reporters may also fail to understand that email addresses and email message "Received:" headers (except for the handoff host) are also usually easily spoofable. This may result in potential false positives if the headers associated with bot-emitted spam aren't correctly interpretted.

Finally, this question might equally well ask, "When detecting bots, is ***collateral damage*** a possibility?"

Collateral damage, or inadvertently hurting a user that isn't botted when dealing with a user that is botted, is a distinct possibility, particularly if users connect multiple systems via a single shared IP address (e.g., by using NAT with PAT). Imagine a situation where an ISP detects bot traffic from its customer's IP, and reacts by blocking that IP. If that IP is shared by multiple downstream customer systems, efforts to block bot traffic from one of those downstream customer systems may unavoidably end up blocking legitimate traffic from other downstream customer systems sharing that same IP address.

***(12) To date, many efforts have focused on the role of ISPs in detecting and notifying consumers about botnets. It has been suggested that other entities beyond ISPs (such as operating system vendors, search engines, security software vendors, etc.) can participate in anti-botnet related efforts. Should voluntary efforts focus only on ISPs? If not, why not? If so, why and who else should participate in this role?***

While ISPs play a potentially pivotal role (since they may be the only ones able to map the IP of a botted host to the identity of an actual customer, and thus may be the only ones able to directly contact a botted customer about their infected status), others do also have roles to play in combating botnets. Efforts should ***not*** be limited just to ISPs.

We've previously mentioned the good work that Microsoft has done with its Malicious Software Removal Tool. Clearly their efforts to directly remove malicious software from user systems with MSRT are tremendously helpful in the fight against bots, as is their program of civil litigation against botnet operators.

Beyond ISPs and Microsoft, one needs to recognize that botnets operate as part of a highly specialized ecosystem. If bots are to be commercially profitable for their operators, a variety of conditions need to be satisfied; disrupting one or more of those conditions may be sufficient to make botnet operation financially unprofitable.

For example, we know that while bots may drive some traffic to spamvertised hosts, additional financially important traffic comes from search engine listings. If search engines delist (or at least "down rank" or "deprioritize") pages from web sites that are being spamvertised by bots (whether that spamvertising is being done by email, web spamming tools, or other means), that sort of technical "penalty" can be devastating to the commercial viability of bot-promoted enterprises.

Similarly, hosting companies also have a role to potentially play: managing botnets, particularly large botnets, requires high capacity/stable servers and substantial bandwidth. That requirement is normally satisfied by botherders purchasing "bullet proof hosting" from complicit (or at least "intentionally disinterested") hosting companies. If hosting companies refused to provide botherders with the facilities they needed for botnet administration purpose, large botnets would be difficult or impossible for botherders to administer. While some hosting companies may be innocent/unknowing victims of botnet operators, hosting companies that knowingly tolerate botnet management servers in their facilities or on their networks need to be held accountable for that business decision. In particular, hosting companies, and any resellers or agents thereof, should be required to have and follow strict 100% "know your customer" policies. Specifically, this means that it should be impossible for a customer to acquire hosting for immediate use without closed loop confirmation of the customer's identity.

Registrars and registries also have a role to play. If the dedicated domain names used for botnet command and control hosts can be disabled/put in "HOLD" status (thereby rendering those domain names unusable), botherders will be hard pressed to maintain control over their botnets using traditional command and control approaches. We also need to ensure that all registries move to a so-called "thick registry model" so that the registry can identify not just ***one*** botnet-related domain, but the ***complete*** set of botnet-related domains that may have been registered to a given botherder with the same (or closely related) registration details.

We also note that miscreants routinely abuse privacy and proxy registration services. Given the levels of abuse associated with such services, we believe that private/proxy registration services should no longer be allowed for commercial enterprises (customers deserve the right to know the identity of the company they may be trading with).

We have no objection to private/proxy registrations continuing to be available for non-commercial registrants, provided, however, that if any non-commercial private/proxy registrant can be demonstrated to be engaging in commercial activity, the private/proxy registration for that putative "non-commercial" entity should immediately be decloaked.

Finally, we would like to see the creation, promotion, sale, distribution or use of bot software be made a separately chargeable felony offense in and of its own right.

***VI. The "Reviewing Effectiveness of Consumer Notification" Section of the RFI***

***(13) What baselines are available to understand the spread and negative impact of botnets and related malware? How can it be determined if practices to curb botnet infections are making a difference?***

When it comes to getting a baseline, and looking to see if efforts to curb botnets are making a difference, look at the statistics available from the Composite Block List, as discussed elsewhere in this response.

You need only look at http://cbl.abuseat.org/domain.html to see examples of some ISPs that are totally overrun with botnets. The cleanest ISPs, and relatively small ISPs don't show up on that page, because they have few if any botted hosts.

In most cases, if anti-botnet measures are effective, infection levels should be less than 0.01% (e.g., for an ISP with a million customers, 100 or fewer customer hosts will be botted at any point in time).

Infection rates that run a full percent or higher (e.g., 10,000 botted hosts per million customers) are typically indicative of ineffective anti-bot measures, or a lack of anti-bot measures.

***(14) What means of notification would be most effective from an end-user perspective?***

Please see our response at section IV. (1) (f) above, discussing approaches for notifying end-users.

***(15) Should notices, and/or the process by which they are delivered, be standardized? If so, by whom? Will this assist in ensuring end-user trust of the notification? Will it prevent fraudulent notifications?***

Bot notices to users need to convey basic information about what's been detected. Standardization may be a side effect of automating notification processes, but will not necessary convey material benefits when notifications are being made to an ***end user***.

When notifications are being made in bulk, from one provider to another, standardization may help the receiving provider automate the ingestion and processing of those notices. See our previous discussion of this point at   
IV. (1) (g), above

With respect to fraudulent notifications, standardization will potentially ***facilitate*** rather than ***deter*** fraudulent notification.

Consider examples from the physical world: letter head stationary can be readily duplicated, and may lend a false air of authenticity to a bogus communication. A police uniform, along with a badge ordered over the Internet, may allow a non-law enforcement person to convincingly "pretend" to be a cop, one reason why impersonating a police office is usually an offense that receives harsh treatment.

Ultimately fraudulent notifications can only be detected and ruled out by reliance on/corroboration with locally collected netflow data (or comparable network data sources of trusted provenance).

If the local network is not well instrumented, providers may want to formally or informally track the accuracy of reports they receive from third parties. That is:  
  
— "Uh oh, we just got another set of reports from Bob in Utah, his previous reports have always proven to be pretty accurate, so we'd better take these seriously as well," or

— "Hmm. Another report from that guy in New Hampshire who thinks our name server is somehow 'attacking' his firewall when he's trying to visit one of user's websites. We've given up trying to explain what's going on to him, haven't we?"

***(16) For those companies that currently offer mitigation services, how do different pricing strategies affect consumer response? Are free services generally effective in both cleaning computers and preventing re-infection? Are fee-based services more attractive to certain customer segments?***

As discussed at IV. (8), above, most commercial malware remediation services ("rent a technical support person"-type outfits) offer three basic models:  
  
— Help at the user's site (they make a "house call" to your home or business, typically the most expensive option)  
  
— Help at the service provider's location (you bring your system to the service provider, the least convenient option,  
 at least for desktop systems)  
  
— They work with you online (this option presumes that your ISP has not cut off your connection, and that malware  
 isn't actively interfering with remediation efforts); this is typically the least expensive option.

Users normally prefer the easiest and least expensive option.

For a rational user who's paying for remediation services out of pocket, the upper bound on what they should be willing to pay for remediation services should be:  
  
 The cost of a new system +

The cost of transferring critical applications and user files from the old system or backups –  
 The expected salvage (resale) value of their old system =   
 The rational ceiling on potential remediation expenses

Users may also perceive an intangible value to buying a new system that may be faster or more reliable or have more features than the old system that it's replacing.

Today's reality, however, is that perfectly serviceable new laptops are available for $500 or less, and desktops are less expensive still. This means that if a user has a severely infected system, particularly one that is now multiple years old, they may be better off replacing that infected system rather than spending hundreds of dollars either attempting to clean it, or executing a nuke-and-pave (format and reinstall) strategy.

With respect to your question in this part about free vs. for-fee services, free services are often not really "free."   
The user may need to devote substantial time and effort ("sweat equity") toward cleaning their system, and those efforts, even if diligent and long in duration, may not assure the user of success. While the user is working on cleaning up their system with "free" resources, they may not be able to spend time working, or enjoying their time off work with their family or friends, and they may not be able to use their system. These are real costs, albeit costs that may be paid in kind rather than in cash.

For-fee services, on the other hand, may allow a specialist to just "do their magic." Like going to the dentist for a root canal, you know that it may be expensive and unpleasant, but sometimes you just need to do what you need to do (assuming you can afford to pay for the work you need).

The downside of bringing your system to a specialist, or a specialist to your system, is that you potentially lose some privacy, and need to trust the technician to do only what they're supposed to do, and to do it well. An untrustworthy computer repair technician who has full access to your system could wreck considerable havoc.

***(17) What impact would a consumer resource center, such as one of those described above, have on value-added security services? Could offers for value-added services be included in a notification? If not, why not? If so, why and how? Also, how can fraudulent offers be prevented in this context?***

Many ISPs may already have established referral relationships with third party for-fee remediation services, and may routinely refer users who need or want extra help to that partner.

The consumer resource center mentioned previously, if created, is unlikely to replace or significantly undercut existing sites of that nature, or the business that currently flows to the private sector for-free security services.

Fraudulent offers can best be minimized by listing links to legitimate sources of computer security assistance on the ISP's web site, and referring the user to that site, or by creating a licensing process, with approved remediation providers listed in a verifiable registry.

***(18) Once a botnet infection has been identified and the end-user does not respond to notification or follow up on mitigating measures, what other steps should the private sector consider? What type of consent should the provider obtain from the end-user? Who should be responsible for considering and determining further steps?***

Ultimately, the ISP has both the authority and the responsibility to deal with its own infected customers.

If infected customers cannot be reached, or cannot or will not deal with their problems, the ISP ***will*** need to take appropriate unilateral measures to limit the impact of the botted customer system to both the ISP itself, and to other users of the Internet. ISPs that fail to do so quickly become "damaged goods:" their IP address space gets listed on block lists, legitimate customers develop deliverability problems, and the ISP acquires a bad reputation. Once that happens, it doesn't take long for good customers to flee, and a deluge of additional bad customers to arrive.

Thus ISPs must take appropriate actions to deal with a botted customer, even if the customer can't be reached, or is non-responsive. This typically means putting the customer in a so-called "walled garden" where the customer's system cannot emit or accept problematic traffic. In extreme cases, or if the ISP has not yet deployed a walled garden, the ISP may end up having to completely terminate the customer's network access. This possibility will typically be provided for in the ISP's terms of service, agreed to by the customer at the time they signed up.

We note that completely terminating a customer's access is generally something that ISPs and customers both want to avoid: terminated customers represent lost revenue, and completely terminating a customer's broadband access may also impact other bundled services, such as cable TV or Voice over IP (VoIP) service.

If VoIP service is interrupted during an emergency period, whether that emergency is a natural or man-made disaster or a medical crisis, there exists a potential for serious injury to persons or property, or even loss of life.

Most ISPs will attempt to limit their liability in those sort of circumstances by either exempting identifiable VoIP-related traffic from broad traffic blocks, or including terms in their terms of service prohibiting customers from exclusively relying on VoIP service for emergency-related purposes.

With respect to the question, "What type of consent should the provider obtain from the end-user?", recall that most ISPs have customers agree to terms of service that give the ISP the right to manage their connection when security issues or other circumstances may require.

Even with that sort of clause, most ISPs will make an affirmative effort to contact the user before blocking their connection. Unfortunately, if a botted user remains persistently infected and/or incommunicado with the ISP, it may not be possible for the provider to contact the user. It is also certainly conceivable that even if the user is able to be contacted, and they objected to being disconnected, an ISP might feel that they have no viable alternative.

Concerning your question, "Who should be responsible for considering and determining further steps?", we believe that ideally the customer should take responsibility for self-monitoring and self-securing their systems. If they fail to adequately do so, ISPs then have a responsibility to act. If the ISP in turn fails, the ISP's upstream network service provider(s), if any, may need to intervene.

However, if the customer, the ISP, and the NSP are all unable to take care of bot-related issues that arise, civil litigation, regulatory action, or criminal law enforcement involvement may be necessary.

Third parties (such as block list operators) may also unilaterally decide to take action against botted hosts at any time in this process, notwithstanding other steps that may be getting undertaken.

***(19) Are private entities declining to act to prevent or mitigate botnets because of concerns that, for example, they may be liable to customers who are not notified? If so, how can those concerns be addressed?***

Liability for failure to notify a customer would imply that an affirmative "duty to notify" exists, as a result of statutory provisions or enabling regulations, or following well-settled common law precedent. We are not aware of any such existing obligation pertaining to notification of botted ISP customers. If a duty to notify ***did*** exist, we'd imagine that a reasonably diligent "best effort" attempt to notify, even if executed imperfectly, would likely result in less liability for an ISP than if that ISP made no attempt to notify botted customers at all.

We would thus always urge ISPs to attempt to notify their botted customers whenever possible, even if they are unable to successfully do so for all types of malware or for every potentially infected customer.

If the departments authoring this RFI believe that some private parties ***do*** perceive potential liability for their anti-bot action, we'd encourage the departments to consider recommending a statutory amendment that would provide a safe harbor for good Samaritans who may be making a best effort attempt to notify botted users.

***(20) Countries such as Japan, Germany, and Australia have developed various best practices, codes of conduct, and mitigation techniques to help consumers. Have these efforts been effective? What lessons can be learned from these and related efforts?***

To empirically answer this, we can look at country level statistics for those countries from the Composite Block List, see http://cbl.abuseat.org/country.html, relative to the United States itself, plus three common comparators, e.g., Canada, the UK and New Zealand:

DE: 13th place 143,066 listed IPs 0.129% infection rate

AU: 58th place 14,009 listed IPs 0.026% infection rate  
JP: 76th place 6,257 listed IPs 0.003% infection rate  
  
US: 20th place 100,980 listed IPs 0.005% infection rate  
  
UK: 35th place 40,731 listed IPs 0.070% infection rate  
CA: 72nd place 7,652 listed IPs 0.009% infection rate  
NZ: 90th place 3,866 listed IPs 0.047% infection rate

In reviewing that table, note that higher rankings, or larger number of listed IPs, are bad, and lower infection rates are good.

When we look at that data, we note:  
  
***(a) The Performance Of Code of Conduct Countries Is Distinctly Non-Uniform:*** There is a huge degree of diversity in rate of infection among the three "code of conduct" countries mentioned.

For example, ***Germany has 43 times the rate of infected IPs that Japan does.***Of course, it's hard to know why such a dramatic discrepancy exists between those two countries, given that both apparently promote best practices, codes of conduct, and mitigation measures.

Perhaps Japanese ISPs are less targeted by malware than German ISPs? Obviously, Japan uses eastern character sets -- perhaps malware hasn't been localized to use Japanese kanji?

That hypothesis is challenged if we note that the world's top two most heavily botted countries, India and Vietnam, collectively accounting for over a quarter of all botted hosts worldwide, both make wide use of non-roman character sets, just as Japan does:  
  
IN: 1st place 1,383,745 listed IPs 3.734% infection rate  
VN: 2nd place 593,169 listed IPs 3.988% infection rate

It is improbable that bots would be able to localize for India or Vietnam, but not for Japan. We can only assume that Japanese ISPs, or their customers, are culturally more inclined to diligently seek out and eradicate bots than their counterparts in India or Vietnam.

***(b) The United States Already Outperforms Two of the Three "Code of Conduct" Countries, and By Significant Factors:*** That is, the United States actually has an infection rate (0.005%) that is over 5X LOWER than Australia (0.026%) and nearly 26X LOWER than Germany (0.129%)

***(c)* *Disregarding Infection Rates, and Just Looking At Raw Bot Counts, the US Still Outperforms Germany:*** Recall that Germany had 143,066 botted IPs while the United States had only 100,980. If a site that's being hit by a botnet only cares about actual bot volumes, and not bot rates of infection, the United States is still less of a potential problem to that target than Germany is.

***(d) Comparing The Code of Conduct Countries against Canada, the UK and New Zealand, There Does Not Appear to Be a Meaningful/Substantive Difference in Infection Rates.*** If we truly want to find comparators particularly worthy of emulation, we might look at the Scandinavian countries as a group -- this five country region outperforms both Australia and Germany.  
  
SE: 86th place 4,357 listed IPs 0.020% infection rate  
NO: 111th place 1,550 listed IPs 0.015% infection rate

DK: 123rd place 1,039 listed IPs 0.008% infection rate   
FI: 129th place 815 listed IPs 0.007% infection rate

IS: 154th place 172 listed IPs 0.023% infection rate

***(21) Are there best practices in place, or proposed practices, to measure the effectiveness of notice and educational messages to consumers on botnet infection and remediation?***

(a) It is hard to teach users everything they need to know about cybersecurity -- even just ***general*** cybersecurity -- much less cybersecurity information about ***specialized*** topics such as botnet infection and remediation.

Cyber security professionals know that user education is hard.

If user education was easy and effective, many security risks would simply disappear: phishing for passwords, and 4-1-9 advance fee fraud schemes, for example, wouldn't work. Users would "get it" and not fall for those hoary old scams. But reportedly, users continue to cough up their credentials, and continue to front tens of thousands of dollars to process the transfer of their "millions" from bogus Nigerian princes.

(b) We also need to recognize that botnets are inherently surreptitious and deceptive -- they do their best to avoid being noticed by users. Given all the tricks that bots can pull, it can hard, even knowing that your system may be infected, to actually detect the presence of the bot, to say nothing of the problems that may arise when attempting to clean an infected system. (Remember, most security experts recommend nuking-and-paving (formatting and reinstalling from scratch, or at least restoring from clean backups, rather than trying to remove malware in-situ).

(c) Remember that many ISPs will insist that their users get cleaned up; enforcement of that policy can make it hard to tease apart effects associated with education and effects associated with policy enforcement by the ISP.

(d) Infection rates are already incredibly tiny -- as mentioned in question 20, previously, only 0.005% of all US IPs are infected. Given that tiny base rate, it may be difficult to accurately measure the penetration and benefit of educational efforts.

***VII. Incentives To Promote Voluntary Action To Notify Consumers***

***(22) Should companies have liability protections for notifying consumers that their devices have been infected by botnets? If so, why and what protections would be most effective in incentivizing notification? If not, why not? Are there other liability issues that should be examined?***

As we've previously discussed at question 19, notification is not normally where liability arises.

When liability arises, if it does at all, is when a provider makes an attempt to help the user get disinfected. Working on a malware infected system can sometimes result in the system crashing or becoming unstable, and it is not unheard of for users to blame a computer technician that's been trying to help them, rather than the malware that's infected their system, if/when that happens.

By comparison, notification is a relatively low impact and low risk activity.

Risks in these and other situations are normally managed with disclaimers: "if you'd like help with your system, be sure you've completely backed it up before you bring it in for work, and please sign this liability waiver before we begin to work on your equipment."

If you'd like to proactively incentivize notification, MAAWG would recommend ensuring that notifications are not a financial burden on firms. That is, if you want notifications to be done, help to pay the costs associated with creating and delivering those notifications, don't make botnet notifications yet another unfunded federal mandate.

***(23) What is the state-of-practice with respect to helping end-users clean up their devices after a botnet infection? Are the approaches effective, or do end-users quickly get re-infected?***

As we've previously mentioned, most security professionals will recommend that an infected system be nuked-and-paved (formatted and reinstalled from scratch, or restored from a clean backup).

If the user doesn't want to do that, or the user lacks the ability to execute that strategy (they can't afford the cost of doing that, or can't find their original media, or they don't have backups of their files, etc.), consumer grade remediation normally involves use of one or more antivirus tools until no more malware is found. (Even then, frustratingly, malware may still be present, albeit unknown to the antivirus softwares that have been used)

If the ISP hasn't licensed a commercial antivirus product, users may be encouraged to try free antivirus products for that process.

That sort of recommendation needs to be made carefully, since some malware authors have released fake antivirus products that may actually infect a clean system, or claim to find malware where none exists. It is MAAWG's belief that production, distribution or sale of fake antivirus malware should be a specifically cognizable federal offense carrying serious penalties, since it attempts to exploit weak users at their most vulnerable, and as such is a particularly heinous and despicable criminal act.

Users who aren't comfortable attempting self-remediation may be referred to a commercial remediation service provider partner, typically a service that the user would need to pay for themselves. As we've previously discussed, the practical upper bound on the cost of such third party work is effectively the cost of a replacement system plus the cost to migrate clean copies of critical files, less the resale value of the old infected system.

You also asked about users becoming re-infected: some do, some don't. The users that take the time to patch their system and take other appropriate steps to harden their system, as we've previously described, tend not to get re-infected. The users who don't take the time to harden their systems, often do get reinfected.

***(24) What agreements with end-users may need modification to support a voluntary code of conduct?***

Most ISP either have a formal contract for service with their customer, or some ISPs may publish terms of service (TOS) on their web site. Depending on the content of a voluntary code of conduct, some terms of those contracts or TOS may require amendment, but it is impossible to say for sure without more information about what might be included in the voluntary code of conduct that's ultimately forthcoming.

***(25) Of the consumer resource scenarios described above, which would be most effective at providing incentives for entities to participate? Are there other reasons to consider one of these approaches over the others?***

Most ISPs are economically rational entities. If you want them to participate in a voluntary code of conduct, ensure that that program nets more revenue than it costs for participants.

Help make the voluntary code of conduct a differentiator, or selling point, that might encourage a reluctant potential ISP to actually sign up. (Maybe offer a web badge of some sort?)

Stress the fact that clean users are easier for the ISP to support, and require fewer system and network resources, and are less likely to defect/be a source of "churn."

But recognize, ultimately, that security is an "order qualifying" characteristic, and not an "order winning" one. That is, people may balk if security isn't present, but few customers put the question, "How security is the ISP?" at the top of their shopping list (they're often more interested in performance, or cost, or features, right?)

***(26) If a private sector approach were taken, would a new entity be necessary to run this project? Who should take leadership roles? Are the positive incentives involved (cost savings, revenue opportunity, etc.) great enough to persuade organizations to opt into this model?***

Most American ISPs already have adopted solutions for managing botted customers, and that's reflected in the low rate of infections in the United States. It's not clear that a new private sector organization is needed, or that it would be successful if created.

***(27) If a public/private partnership approach were taken, what would be an appropriate governance model? What stakeholders should be active participants in such a voluntary program? What government agencies should participate? How could government agencies best contribute resources in such a partnership?***

Many public/private sector partnerships have been tried over the years; in the security space, two of the most widely known ones are probably the FBI's Infragard program, and the various DHS critical infrastructure sector Information Sharing and Analysis Centers, or ISACs.

What we know from those experiments is that some Infragard chapters thrive, while others wither or become vestigial. Likewise, some ISACs are well subscribed and do important work, while others exist in name only.

The telling factors that seem to distinguish the programs that succeed from the programs that fail are usually:  
  
— The partnership must have real/important work to do, work that's valued by the participants

— A critical mass of participants must be available in the geographic area (an agriculture ISAC in Manhattan   
 might be expected to fail, for example, given the limited number of urban farmers)

— Participants need to be trusted, and prove worthy of that trust

— Usable information sharing channels (mailing lists, meetings, etc.) must exist

— Information sharing needs to drive action

— Information sharing needs to be bidirectional

— Agency support must be genuine, and not pro-forma

— You need steady management with a light touch

Governance, whether for a thriving or failing organization, commonly involves a governing board plus an executive director or co-executive directors. (In many respects, if the organization is otherwise sound, governance participants may find themselves with little work that needs to be done.)

You asked, "What stakeholders should be active participants in such a voluntary program?"

As a voluntary program, participation should be open to all trustworthy ISPs or individuals. Whether those entities elect to actively participate or not will be up to them.

You also asked, "What government agencies should participate? How could government agencies best contribute resources in such a partnership?"

It's not clear that any existing government agency is completely "right" for the envisioned activity.   
  
— Remediation of botted end user systems is not really a core law enforcement mission element, although law   
 enforcement has a role in investigating and prosecuting bot herders and bot users.   
  
— Participation by members of the intelligence community may make some non-governmental participants anxious   
 or reluctant to share, and in most cases sharing of data from the intelligence community to uncleared   
 participants would be difficult or impossible.  
  
— US CERT might be a suitable participant, but they may not have sufficient resources (particularly if a   
 distributed model is employed) to effectively do so without compromising higher priority responsibilities  
  
— The FTC mission really isn't aligned with tackling bots, and their experience with tackling spam has shown  
 that they're under-resourced to tackle their existing portfolio

— The FCC has historically had regulatory responsibilities with respect to some potential participating actors,  
 but that regulatory history may negatively color, or provide an appearance of coercion, for what is meant to  
 be a voluntary program

— Perhaps the Office of Justice Programs might work? They have grant programs that are intended to leverage  
 technology to fight crime (see http://www.ojp.gov/programs/technology.htm ), although admittedly their normal  
 focus is on justice-related entities, not ISPs.

When it comes to contributions from any agency that does participate, natural expectations will likely be:  
  
— resources (funding, facilities (such as meeting rooms or servers), staff flywheel support),

— information (e.g., unclassified intelligence sharing), and

— action on information shared from the private sector ("I've identified a botnet C&C, and its located in Chicago...").

***(28) If a government-run approach were taken, what government agencies should play leading roles?***

See the discussion of agencies in the preceding question.

***(29) Are there other approaches aside from the three scenarios suggested above that could be used to create a consumer resource and to incentivize detection, notification, and mitigation of botnets?***

We would urge you to be clear on one potential customer population (or audience segment) that might need help: there are some users who are botted, and who have exhausted all free resources, and who may not be able to afford to purchase commercial remediation assistance, and who may also not be able to afford to replace their infected system.

Where are those economically disadvantaged users to turn?

If we simply throw up our hands, and say, "Sorry, your infected system is your problem, not ours," we may come to regret that decision.

If left infected, those botted systems can be turned against any or all of us: attacking government agencies, DDoS'ing critical infrastructure, or getting used as a stepping stone from which to hack defense industrial sites or even foreign countries.

Those economically disadvantaged users need help to get cleaned up.

As in most things where all other resources have failed to successfully tackle a problem, the government may be all that's left, acting as a party of last resort, just as it does when it confronts the results of floods, hurricanes, or earthquakes.

That role, this "safety-net" function for the systems of our poorest citizens, would require distributed service centers, since most poor people may have little or no ability to transport themselves or their systems for help.

We also need to recognize that while we want and need to help our ***own citizens*** who have run out of options for cleaning up their infected systems, many of the botted hosts that routinely attack Americans are located ***outside our borders***. We also need a plan to help clean and correct THOSE systems, not just domestic ones.

One of MAAWG's Senior Technical Advisors has previously shared some thoughts on these requirements, see  
"We Need a Cyber CDC or Cyber World Health Organization,"   
http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf

***(30) Are there other positive incentives that do not involve creation of an organized consumer resource that could encourage voluntary market-based action in detection, notification, and mitigation of botnets?***

Consider offering a cash bounty program that would pay a reward for each new botted host that's identified (and accurately reported) with evidence supporting the report. A bounty program of this sort would directly encourage private parties to identify and report the bots they encounter.

Also consider creating an application that users could run, which would voluntarily associate a contact address supplied by the user with the IP address that the user is using. A blind remailer could then forward mail from authorized reporters to those email points of contact if a particular IP address appeared to be botted or otherwise have issues. This application would allow ISPs to be taken out of the role of acting as a critical conduit (e.g., it would no longer have to connect an IP address which is having issues to a customer, the customer could be contacted directly, but in a secure and privacy-preserving way).

**Conclusion**

Thank you for this opportunity for MAAWG to comment on " Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware". If you would like us to discuss any of our remarks in more depth, or if you have any questions, please do not hesitate to contact us.

Sincerely,

/signed/

Jerry Upton, Executive Director

Messaging Anti-Abuse Working Group

jerry.upton@maawg.org

http://www.maawg.org