From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 17th, 2010
Subject: Comments on "Cybersecurity, Innovation and the Internet Economy," Docket No.: 100721305-0305-01

Introduction

Thank you for the opportunity to review and submit comments on the Department of Commerce's ("DoC") request for comments relating to "Cybersecurity, Innovation and the Internet Economy," (hereafter, "the DoC request"). [1]

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 as well as from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (www.MAAWG.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and the facilitation of collaboration.

MAAWG commends your goal of:

> "develop[ing] an up-to-date understanding of the current public policy and operational challenges affecting cybersecurity, as those challenges may shape the future direction of the Internet and its commercial use, both domestically and globally."

MAAWG agrees and notes that MAAWG member companies confront those same challenges every day. As these remarks are reviewed, we appreciate consideration of our members' insights as you plan future DoC cybersecurity programs.

The DoC request invited respondents to address eight fundamental areas relating to cybersecurity:

i) Quantifying the Economic Impact
ii) Raising Awareness
iii) Web Site and Component Security
iv) Authentication/Identity (ID) Management
v) Global Engagement
vi) Product Assurance
vii) Research and Development
viii) An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

We will offer comments in most of those areas in the order presented, with the exception of the product assurance area.

Area 1: Quantifying the Economic Impact

The DoC request stated "[...] it appears difficult to assess the macro- and microeconomic impact of cybersecurity incidents with current tools" and "The availability of authoritative, aggregated data on cybersecurity investments and losses from cyber incidents might yield a quantitative picture of the economic impact of cyber intrusions and attacks." [2]

MAAWG agrees that it is important for the Department to be able to quantify the economic impact of cyber intrusions and attacks. Correct programmatic decisions cannot and will not be made unless the magnitude of the cybersecurity threat is correctly understood.

However, we respectfully disagree with the assertion that required tools or data are lacking to provide at least a lower bound on the economic impact of some types of cyber abuse, such as spam. One estimate for the cost of spam was provided by Ferris Research. Their 2009 estimate put the worldwide cost of spam at $130 billion USD, with spam in the U.S. alone costing $42 billion USD. [3] Losing over $40 billion USD to spam is a huge drag on the American economy, although most of us have a hard time comprehending

numbers that large since they are simply not very common. Economic numbers of that magnitude usually arise only in the context of major disasters. For example, Hurricane Katrina in 2005 was a roughly $100 billion USD disaster. [9] We do not mean to imply that spam is, or could be, anywhere near as directly devastating as Hurricane Katrina when we consider the human suffering associated with that disaster, but we must recognize that two to three years of spam can cause an aggregated national *economic* impact that is roughly comparable to the loses associated with that major storm.

Given the magnitude of that loss, why has spam and other cyber-abuse not been put squarely in the federal cross hairs for immediate priority action? Many perceive spam to be a diffuse, chronic, low-intensity threat; a threat that is popularly perceived to be "just an annoyance" that we all abhor but nothing more serious than that. Once the community recognizes that two to three years of this "annoyance" has caused a hundred billion dollar drain on this country, perceptions will change and spam will go from being “just an annoyance” to being a huge problem that demands immediate attention from the Administration.

There are also many other perspectives to view this issue. For example, consider tangible ISP and enterprise IT operational costs for essentials such as email server capacity and network capacity. The MAAWG Email Metrics Reports [10] make it clear that abusive messaging consistently accounts for 88% to 92% of all email sent through the Internet. Based on this, we can assume 90% of all email traveling the Internet is unwanted. Again, to put this in context, for every mail server or gigabit of network capacity or terabyte of disk space that an ISP might provision to service the actual messaging requirements of its customers, it must *also* potentially buy nine more just to "throw away" on spam and other unwanted message traffic. [11] That represents a huge cybersecurity "tax" on struggling ISPs.

These two examples illustrate that we already have at least some ability to estimate the impact of messaging abuse on the economy and the impact is immense. What we need is appropriate federal action by relevant federal agencies to help the private sector address this chronic problem.

Area 2: Raising Awareness [e.g., Cybersecurity Education and Training]

In this section the Department mentioned, among other statements, they "[are seeking] comment[s] on the efficacy of existing [cybersecurity] educational efforts, as well as steps that might be taken to improve them" while also asking, "Who should be the target audiences?" [12]

The cybersecurity threats that consumers and small businesses currently face are overwhelmingly complex and are constantly changing. Even cybersecurity professionals who focus exclusively on this area find it difficult to stay fully aware of all the known and emerging threats arising on all platforms. It is not realistic to expect typical consumers to attain even a fraction of that level of professional expertise; yet without that expertise, they will likely be unsuccessful at selecting appropriate measures to protect their systems in their homes and businesses.

Consider, for example, traditional consumer-level advice such as, "Keep your system patched, use an anti-virus product, and install a firewall." That advice was good in its day, but is no longer enough.

Now, even if users manage to successfully keep Microsoft Windows™ , Microsoft Internet Explorer™ and Microsoft Office™ patched, they may still have numerous other unpatched third-party applications that can be successfully exploited by cyber criminals to compromise their systems. [13] To stay safe, users and small businesses need to keep all their applications updated; an attacker's automated tools only need to find one application that has not been patched to successfully compromise a targeted system.

Similarly, signature-based anti-virus software once provided substantial protection against the malware commonly seen in the wild, but now miscreants are successfully overcoming signature-based anti-virus solutions. Criminals now routinely tweak and repack their malware faster than anti-virus vendors can keep up. Thus, while signature-based anti-virus software still blocks some threats, and should continue to be used to block what it can, we need to recognize that malware will routinely evade or overcome it.

The advice to "install a firewall" was substantial when the threat was largely from external attackers scanning and probing huge portions of the Internet. However, contemporary attacks are more likely to come from trusted sites the user is already accessing, sites whose content (including malicious content) is routinely allowed to pass the user's firewall unhindered.

What, then, should a consumer education program tell consumers? Clearly, simple advice is no longer effective and obviously more complex guidance is too daunting for most consumers to apply effectively. The goal here is to devise consumer education that makes

comprehensive solutions accessible or even attractive to the average user. We believe there are, in fact, multiple educational opportunities that represent "low hanging fruit":

a) Users want advice on how to better protect themselves online and what to do if their personally identifiable information has been compromised. Small businesses need help, too.

Americans are worried about their online safety, particularly the safety of their personal and financial information. [14] Users are particularly ready for simple and practical advice they can follow to help them stay safe online, including information about what they should do if they are the victim of a breach. While it can be challenging to craft a message that is effective yet comprehensible, this appears to be an area where users are open to well-crafted advice.

We also note that businesses, particularly small businesses, also need advice in this area. They want to keep their customers' personally identifiable information safe but detailed recommendations (such as the Payment Card Industry Data Security Standard (PCI-DSS) version 1.2.1 [15]) may be overwhelming for businesses with limited in-house IT staffing. For example, the PCI-DSS v. 1.2.1 currently spans 74 pages. The advice in that document is excellent but may require time and resources not available to small businesses and entrepreneurs.

b) We need to attack miscreant profits by going after their potential customers.

Currently, virtually all spam is economically motivated and in most cases, in order for spam to yield a profit for the spammer, customers need to purchase a service or product (such as illegal pharmaceuticals, pirated software or knockoff watches). [16] Spammers have no incentive to continue if customers do not purchase those products or services. Unfortunately, little – if any – attention is currently spent on "anti-marketing" measures or efforts to undercut the viability of "spamvertised" products or services.

For example, the DoC might establish a program of public service announcements (PSAs) addressing issues like spamvertised pharmaceuticals. The message should be kept simple and clear and target general public audiences; perhaps as simple as:

> He's not Canadian.
> He's not a pharmacist.
> His pills aren't real.
> Don't buy spamvertised pills.

This is a simple message but one that could potentially turn illegal pharmacy spamming into an unprofitable exercise.

c) We need to remind users that plain text is safe.

Many of today's threats rely on exploitable vulnerabilities in complex protocols, yet users routinely use those complex protocols even when simpler protocols are all that is needed. For example, often basic documents, such as a simple meeting agenda, is sent as a formatted Microsoft Word™ document, even when a simple plain text message would have worked equally well and not serve as a potential vector for delivering malware. If users are encouraged to use plain text whenever they can, their risk of being infected by malicious email via dangerous HTML constructs or malicious attachments can be at least incrementally reduced, although as NIST notes in *Guidelines on Electronic Mail Security,* [17]

> Limiting the use of HTML within email, such as requiring users to send and view emails in plain text only, has security benefits but can seriously impact functionality for users, such as causing graphics, hyperlinks, and other HTML-based content to be disabled or suppressed altogether. Some organizations choose to block all HTML-based email because they have decided the security benefits outweigh the loss of functionality.

Note that we are *not* recommending that organizations impose a blanket ban on all non-plain text email, only that users be encouraged to use plain text when they can do so without causing a loss of required functionality.

As a second example, consider Web pages that require users to run with scripting enabled in their browsers to access the contents of that page. While scripting enables powerful and attractive new interactive Web-based applications, it also is a prime technology used by miscreants to compromise user systems. We recommend the following advice for site designers who want their users to be safe online by avoiding known attack vectors: Do not make users enable scripting just to use online banking sites or other sensitive websites. Public awareness campaigns can, and should, be used to promote fast, simple and secure websites as an alternative to today's often slow, complex and insecure ones.

d) Many of our domestic cybersecurity problems are enabled by compromised systems abroad, although we also need to deal with material issues at home.

When we think about cybersecurity education and awareness, we must recognize that many of the cybersecurity problems we see in the United States are enabled by insecure systems overseas. For example, looking at the geographic distribution of the 9,274,224 botted hosts listed on the Composite Block List ("CBL") as known sources of spam, [18] the top eight countries account for over half of all the known compromised systems worldwide:

1) India	1,433,021	15.45% of the total	15.45% cumulative
2) Brazil	1,202,415	12.97%	28.42%
3) Russia	557,989	6.02%	34.43%
4) Vietnam	540,096	5.89%	40.32%
5) Ukraine	289,801	3.12%	43.45%
6) Germany	274,339	2.96%	46.40%
7) Italy	244,847	2.64%	49.04%
8) U.S.	241,158	2.60%	51.64%

This distribution of botted hosts is important because it tells us where the need for cybersecurity user education is greatest. It also directs us to where we might potentially see the greatest return for each user-education dollar expended.

In part, this means making sure our own house is in order: Being listed as having the eighth highest number of "botted" (compromised) hosts in the world undermines our credibility and our ability to lead by example abroad. We should be working to lower America's population-normalized level of compromised hosts, which is currently 241,158 botted hosts from a population of 310,233,000, or a rate of one botted host for every 1,286 American persons. This should be reduced to the sort of levels seen for Japan, which is 10,573 botted hosts from a population of 126,804,000 persons, or a rate of one botted host for every 11,993 Japanese persons. Doing the math, that would mean that we should be working to have fewer than 26,000 botted hosts countrywide, rather than our current 241,158 botted hosts.

While we certainly must make progress in getting our own 241,158 compromised systems secured, we will likely see *more* net improvement if we can begin to help the BRIC [19] nations get their millions of compromised systems under control. We routinely provide a variety of foreign aid (including security assistance) to other countries, so perhaps we could offer effective *cybersecurity*-related foreign aid to help our friends abroad who are being victimized by cyber criminals.

The most abused countries are the ones that most need effective consumer awareness efforts *and* language-appropriate cybersecurity resource materials. Many key cybersecurity software tools and documents are currently only available in English, which may be as effectively inaccessible and unusable to non-English speaking users in other countries as documents in Chinese would be to most Americans.

e) Once users are aware of security issues, they need somewhere to turn for trustworthy and affordable technical help.

It is one thing to raise user awareness about the importance of cybersecurity, but once users are attentive, where can they turn for help? Many users want to secure their systems, but they do not have the specialized expertise, tools, money or time to clean and harden those systems. Commercial firms offering cyber clean up and hardening services may cost more than the cost to replace some systems outright. [20]

We have many federal assistance programs for those who need help in many other areas, but we have nothing when it comes to federal cybersecurity assistance for those who cannot afford commercial help securing their systems. We need a federally funded "cyber help" option where consumers or small business users can take their infected systems and get assistance for low or no cost once they realize they have problems. This is a concept that has previously been discussed. [21]

f) The federal government has cybersecurity information that might be valuable to private sector security practitioners, but which it cannot share because of information classification issues.

Much of the most helpful and directly useful cybersecurity information concerns current threats. That information is typically classified when it originates from federal sources, and this keeps it from being shared with those in the private sector who could use the information to protect their systems. For example, consider the following quote from Amit Yoran, former head of the Department of Homeland Security's Cybersecurity Division [22]:

> When you have information that's tightly controlled, you don't have the type of information sharing broadly among different operators. So the intelligence community isn't sharing information with the folks who run systems or with the private sector and people are at a loss - they don't understand the threat environment and what they need to do to protect themselves. They're uninformed about risk management practices. The result? They get compromised and leak intellectual property. So, at a policy level, that's difficult. At an operational level, you have IP addresses and information about exploits that are classified and can't be uploaded to unclassified systems for analysis. That's a very sensitive issue that hasn't been significantly changed since the Bush era.

There is no program by which cybersecurity practitioners can voluntarily request consideration for a security clearance, even if they are willing to pay the cost of conducting that clearance. [23] This lack of security clearances, and the lack of an avenue whereby relevant individuals can correct that deficiency, directly and continually inhibits public/private sector collaboration on operational cybersecurity issues.

The Department of Commerce should consider offering a voluntary pilot program whereby suitable cybersecurity practitioners can be identified and invited to request a clearance. These cleared practitioners would be potentially eligible to receive access to classified federal cybersecurity information.

g) We need to break the cycle of cyber insecurity by training the next generation today.

If all schools included at least fundamental cybersecurity instruction for elementary, middle school and high school students, we would be well positioned to insure that the next generation of computer users has a sound foundation for cybersecurity when they are adults and employees or business owners. Many schools already endeavor to do this using locally developed materials or model curricula such as “CyberSmart!”. (See http://cybersmartcurriculum.org, a program endorsed by the National Cyber Security Alliance, the National School Boards Association, and other educational leadership organizations.) Unfortunately, cybersecurity training is still far from ubiquitous. Support and encouragement from the Department of Commerce in partnership with the Department of Education could go far to broaden the adoption of cybersecurity education in K-12.

Area 3: Web Site and Component Security

In the third part of the request for information, the Department of Commerce asked:

> Should the government alone, the private sector, or the government and the private sector collaboratively explore whether third-party verification of Web site and component security is or can prove effective in reducing the proliferation of malware? If so, what measures should be considered? What would be the implementation challenges in deploying such measures?

Multiple projects already collect and distribute information about malicious and unwanted software and where it is located on the Web. Just to mention a few such efforts (in alphabetical order):

- AMaDa (abuse.ch Malware Database) [24]
- BLADE (Block All Drive-By Download Exploits) [25]
- Clean MX [26]
- DNS-BH - Malware Domain Blocklist [27]
- hpHosts [28]
- Malcode Database [29]
- Malware Patrol [30]
- Paretologic URL Clearing House [31]
- Threat Log Dangerous URLs [32]

There are almost certainly other such projects not listed here. Our intent in listing these projects is not to provide an exhaustive list of sites tracking malware, but simply to provide evidence there are already multiple projects engaged in identifying and documenting Web-borne malware, although in some cases malware-dropping sites may only be identified and added to these sites some time after they initially get deployed.

Nonetheless, substantial information about Web malware is available in "productized" ways that can help to protect end users and small businesses on the Web. For example, there are options such as:

- Built-in browser malware safety features (or third-party plugins or add-ons), [33]
- Filtered DNS services [34], and
- Filtered Web proxy gateways [35]

The more difficult questions relating to Web-born malware, which this notice of inquiry did not ask, are questions such as the following:

- Once we have identified malicious pages on the World Wide Web, can we get those malicious pages taken down? If we find vulnerable servers or applications (which will inevitably be found and exploited by malicious actors), can we get those vulnerable servers patched and hardened?

  What if malicious pages are hosted by so-called "bullet proof hosting" sites, sites which promise (for additional financial consideration) they will simply ignore any complaints they may receive?

  Or what if malicious pages are hosted using “fast flux” or “double flux” techniques [36] and the domain name registrar and registry are unwilling or unable to assist in taking those domains down?

- There are also conflicts between the security and privacy that end-to-end encryption provides and the network operators’ ability to protect users against malware via network-based anti-malware solutions such as Web proxy gateway devices.

  Network-based anti-malware solutions may have difficulty with end-to-end encrypted (aka "secure," "https," "SSL" or “TLS") Web content because the network gateway may not be able to observe that network traffic unless it breaks the end-to-end security model by acting as a "man-in-the-middle" to obtain access to the otherwise opaque encrypted traffic flows. Web anti-malware gateways also may not have visibility into IPSec VPN traffic or IPv6 tunneled traffic, for example.

- More generally, are we willing to architecturally abandon Internet transparency [37] and the end-to-end model in an effort to block Web-based malware via inline devices? Or, above all else, should we strive to preserve a fast and simple Internet that does not interfere with future generative innovation?

The biggest issue, however, is that there is no government entity with the ability to compel an ISP, NSP, or registrar to take down a known malicious Web page. Any process that requires litigation or other protracted formal legal process would likely be too slow to effectively address these threat vectors.

Thus, takedowns are often purely a matter of voluntary action on the part of an ISP, hosting company, registrar or registry. Their willingness to do takedowns – and to risk potential legal action as a result of taking a believed-malicious page down – is far from universal. Because of this, the biggest "hammer" that incents compliance is likely the risk of being block listed by Spamhaus [38] or other private blocklist operators.

ISPs, hosting companies, registrars and registries should be encouraged to protect themselves and the Internet by adopting strong terms of service and enforceable acceptable use policies. Having done so, they will have a sound contractual legal footing that will allow them to respond quickly and effectively when confronted with abuse.

Area 4: Authentication/Identity (ID) Management

Because MAAWG recently commented on the National Strategy for Trusted Identities in Cyberspace (NSTIC), [39] we will not be offering further comments on this topic here.

Area 5: Global Engagement

In this area, DoC asked for feedback on, among other questions, "[...] other cybersecurity-related problems U.S. businesses may be experiencing when attempting to do business in foreign countries." [40]

There is no question that due to the “flat” any-to-any nature of the Internet, cyber crime and cybersecurity are global issues. What happens (or does not happen) in Brazil, Russia or India can directly affect those of us in Washington, D.C. or Los Angeles or London or Tokyo. Spammers and other cyber criminals know that by working globally they complicate the process of identifying and combating their malicious activities. Their transnational operations inject a variety of complications, including issues relating to diversity of jurisdictions and differences in national laws, language-related complications, and even problems due to time zones (scheduling meetings when participants may be halfway around the world can be quite challenging). Spammers and other cyber criminals revel in all the problems their international operations can produce.

While MAAWG is a global anti-abuse organization, our meetings and membership to date have largely been North American and European, albeit with growing Asian participation. Our ability to engage effectively with our anti-abuse colleagues in the Southern Hemisphere has been limited by the sheer distance and costs involved, notwithstanding the fact that members of the messaging community in Peru or Pretoria or Perth share many of the same cybersecurity challenges as users in Pasadena or Prague.

Our ability to resolve common messaging security problems with a global voice is adversely affected when we lack truly global participation. This theme is one that the Internet Corporation for Assigned Names and Numbers (ICANN) and the Department of Commerce itself has experienced while acting as steward of global Internet resources such as Internet names and numbers, but it is also an operational challenge for those of us focused on cybersecurity and combating messaging abuse.

Other federal agencies, such as the Federal Bureau of Investigation, have formal programs intended to insure they have representation *on the ground* in relevant foreign locations. In the FBI's case, this program is known as the "Legal Attaché" or "Legat" program. [41]

We also know that the State Department routinely has commercial attachés located at major embassies and consulates abroad. These attachés have done fine work facilitating international trade.

It is not clear whether or not the State Department, or the Department of Commerce itself, has equivalent representation abroad with the specialized expertise necessary to professionally address *cyber issues* of concern to the Administration and to American businesses. If not, perhaps the Department should consider having its own specialized, technical "boots on the ground" abroad, staffed by career employees with specialized cyber knowledge and expertise.

We recognize that deploying international Department of Commerce cyber business officers is a programmatic option that may take time to evaluate and implement. In the meantime, the Department may want to take other steps to increase its international engagement on cyber issues.

The Internet Engineering Task Force (IETF), the network's leading technical forum for developing and promulgating Internet-related standards, meets at international locations on a rotating basis three times a year. For example, IETF 76 was held in Hiroshima, Japan, IETF 77 was held in Anaheim, California, and IETF 78 was held in Maastricht, Netherlands. We would encourage the Department of Commerce to consider hosting an international cybersecurity summit immediately after each of the IETF meetings, in the same city where the IETF is held, thereby maximizing the opportunity for technically knowledgeable individuals from the international community to "stay over" following a meeting they are already attending. This would provide an opportunity for some of the Internet's best and brightest contributors to participate in cybersecurity-related discussions while minimizing international travel expenses and making the best use of their time.

Collocating such a meeting with the IETF would also increase the likelihood that participants in a DoC cybersecurity summit event would be exposed to the standards-setting process as employed within the IETF. This exposure would help to facilitate your stated goal of "better encourag[ing] the use of internationally accepted cybersecurity standards and practices outside of the United States."

What else might the Department consider in terms of global engagement on cybersecurity?

The United States, along with 42 other nations, has signed the international Council of Europe Convention on Cybercrime. [42] Obviously, that means that over 150 other nations still have not. While the COE Convention on Cybercrime is not perfect, it does provide at least a framework for progress on international cybercrime issues and should be encouraged as an important first step toward making cybercrimes illegal worldwide.

Area 6: Product Assurance

MAAWG will not be offering comments on this topic.

Area 7: Research and Development

The request for comments asked:

> How can the federal government best promote additional commercial and academic research and development in cybersecurity technology? What particular research and development areas do not receive sufficient attention in the private sector? What cybersecurity disciplines most need research and development resources (e.g., performance metrics, availability, status monitoring, usability, and cost effectiveness)? How effective would a federal government-sponsored "grand challenge program" be at drawing attention to and promoting work on specific technical problems?

We view research and development funding for cybersecurity as critical and encourage the Department to continue (and increase) funding for research and development work in this area. This is particularly important in the area of messaging abuse as well as in areas relating to emerging technologies such as IPv6.

That said, while this question appears to be asking for some fairly specific advice, rather than offering a snapshot (that will only be helpful for a brief moment), we instead are recommending a process change that may deliver lasting value for the Department. Many federal research and development projects are fairly abstract and often are not well grounded in the empirical setting of commercial-scale operational realities. As a result, fairly peripheral or irrelevant questions may end up extensively studied or "solutions" may end up being developed which have little chance of being adopted and deployed Internet-wide.

To help avoid this problem, we encourage the Department to convene a standing cybersecurity research technical advisory board with representation from actual Internet operators, cyber law enforcement entities, and leading anti-cyber crime groups. (MAAWG would obviously be pleased to participate in such an activity, if invited to do so.)

A DoC cybersecurity research technical advisory board could provide ongoing programmatic advice to the Department on a variety of cybersecurity research and development issues, including identifying problem areas which are most in need of R&D funding from an operational point of view and providing feedback on approaches which will likely actually be operationally deployable. Such a board should also be explicitly charged with facilitating researcher access to appropriately anonymized data from Internet operators [43], thereby insuring that researcher-developed models are faithful to documented reality and proposed protocols will work when deployed in the real world.

At the same time, taking a long-term perspective, while the Department of Homeland Security's *Roadmap for Cybersecurity Research* [44] correctly identifies current "hard problems" in information security research, there may be insufficient financial rewards to motivate the research community to focus on those long-term, high-risk/high-reward areas. The DoC may wish to partner with DHS in offering "X-Prize"-like [45] financial incentives to catalyze attention on these cybersecurity "grand challenges," and to reward measurable objective achievements in advancing cybersecurity research in these crucial (but difficult) areas.

Area 8: An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

In this last section of the request for comments, [46] you asked:

> Do particular business segments lack sufficient incentives to make cybersecurity investments? If so, why? What would be the best way to encourage businesses to make appropriate investments in cybersecurity? Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make such security investments? Are there disincentives that inhibit cybersecurity investments by firms? If so, what should be done to eliminate them?

As an example of an addressable problem that lacks incentives, consider the problem of "spoofed" network traffic. All network traffic has an IP source address and an IP destination address. An ISP knows what IP addresses have been allocated or assigned to its network, and network engineers could install filters at the ISP's border routers to prevent emission of traffic that has been created with

someone else's source addresses (a "spoofed address") rather than the real address. This sort of network ingress filtering is defined and recommended in a well-established Internet standard known as “BCP 38.” [47] We know, however, from research done by the MIT Spoofer Project that approximately one quarter of all autonomous systems [48] still allow emission of spoofed traffic. [49]

So why do roughly one in four networks still allow spoofed traffic to be emitted? When considered from a superficial and self-interested point-of-view, the answer is simple: While filtering abusive traffic helps make the Internet a better place for everyone else, it does not help the network operator itself be more secure. It does, however, add complexity and additional costs.

This asymmetry of costs and benefits is not restricted just to spoofed network traffic; it also applies to spam from botted hosts. [50] Botted hosts that send spam generally do not send that spam to servers on their same network; they usually target servers elsewhere. Thus, if an ISP cleans up its own botted customers, it does not reduce the amount of spam it receives; rather, it reduces the amount of spam other people may receive. Therefore, intuitively, cleaning up botted hosts is an altruistic action rather than an economically rational one.

On the other hand, operators know that if they do not run a clean network, spam from their networks may result in their address spaces or domains being block listed. Once they are block listed, their traffic – even their legitimate traffic – will be shunned by the community. Thus, there are costs to the operator's *reputation* that actually do provide an economically rational basis for committing resources to running a clean and spam-free network.

This appears to contrast the BCP38 case. The difference is that unlike widely used anti-spam blocklists, such as those run by Spamhaus, there are no blocklists that specifically focus on networks that choose to allow spoofed IP traffic to be propagated. The problem is that currently no one (except the researchers at MIT) is paying much attention to identifying the networks that are running "loose ships" where spoofed traffic can be emitted.

What is needed is more and better access to information identifying those networks. Information is the key to many cybersecurity problems because with information we can make informed decisions when mitigating risks.

Another example of this can be seen in the area of domain names. As a result of lax attitudes toward abuse (or for other reasons), some registrars and domain name resellers are known to be disproportionately popular with spammers and other cyber criminals. Normally this would result in domains from those registrars acquiring a negative reputation, and that negative reputation would result in appropriate site-by-site action. However, when it comes to domain names, there are not scalable ways to identify the set of all domains that belong to a given miscreant-preferred registrar. We lack transparency; we lack information.

One particularly noteworthy manifestation of the current lack of transparency can be seen in the poor condition of the Internet’s “whois” systems. [51] The January 2010 Whois study conducted for ICANN by NORC [52] found that only 23% of the domain whois records it examined were fully accurate. A mid-2009 IP whois point of contact study done by ARIN (the American Registry for Internet Names and Numbers) [53] involved sending verification messages to 29,929 IP whois point of contact addresses, addresses that should be monitored and answered by resource holders; out of the nearly 30,000 queries sent, only 1,192 responses were received, a dismal response rate of just 3%.

If the Department wants to do one thing to help ensure that network reputation mechanisms work the way they should, it should take steps to increase transparency and accuracy with respect to the Internet names and numbers it oversees. Let people have access to the data they need, while striving to make that data as accurate as possible. The community can then make informed decisions about their online neighbors and the Internet community will take it from there, implementing appropriate protections for their networks and users.

Conclusion

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

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

References:

[1] "Cybersecurity, Innovation and the Internet Economy," Fed. Reg. Vol. 75, No 144, pp. 44216 et. seq., www.ntia.doc.gov/frnotices/2010/FR_CybersecurityNOI_07282010.pdf

[2] "Cybersecurity, Innovation and the Internet Economy" at pp. 44219.

[3] Ferris Research, January 28th, 2009, www.ferris.com/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions/

Is that Ferris Research estimate credible? Could we *really* be losing as much as US $42 billion a year to spam?

If an employee or consumer has ineffective or no spam filtering, those individuals will waste time every day identifying and deleting messages they should never have received in the first place. Even users with *good* spam filtering will still find themselves losing time due to spam, if only as a result of needing to dredge through their spam folder looking for real mail that may have gotten miscategorized as spam or as a result of needing to confirm that recipients they have sent mail to have actually successfully received it. Without spam, these costs would not have been incurred. The costs associated with spam, while small on an individual basis, becomes huge when considered in the context of hundreds of millions of American Internet users.

Email usage is ubiquitous among Internet users. If we assume that the average American Internet user receives a couple dozen spam per day [4] (considering all their accounts and media), and they spend on average five seconds per spam dealing with each one, that means the average time lost to spam is two minutes per American Internet user per day (24 spams per day x 5 seconds per spam / 60 seconds per minute). Now multiply that by the number of American Internet users:

US Population, September 3rd 2010:	310,159,546 [5]
Percent of the population that is 18+:	75.5% [6]
Fraction of Americans using the Internet:	77.3% [7]

	181,013,763

Let us round that value to 180 million adult American Internet users. If each of those users wastes two minutes per day, it means that we waste 360 million minutes per day on spam. That is the equivalent of 750,000 wasted eight-hour workdays (360,000,000 minutes/(8 hrs per work day x 60 min per hour)) each and every day, day in and day out, year round.

What is that loss in US dollar terms? The Bureau of Labor Statistics quotes the average hourly earnings at US $22.66. [8]

Multiplying 8 hours/workday x US $22.66/hour x 750,000 workdays x 365 days/year works out to roughly US $49.6 billion/year. That value is quite consistent with the Ferris Research estimate of US $42 billion/year.

[4] "2nd Annual Spam Report: Cost of Spam More Than Doubled in Past Year to $1,934 Annually Per Employee," http://nucleusresearch.com/news/press-releases/2nd-annual-spam-report-cost-of-spam-more-than-doubled-in-past-year-to-1934-annually-per-employee/ mentioning "The average employee receives nearly 7,500 spam messages per year [in 2004], up from 3,500 in 2003." 7,500 spam per year / 365 days per year = 20.5 spam per day. We round that up to two dozen spam per day based on the conservative assumption that spam has gotten substantially worse since 2004.

[5] US Population Clock, www.census.gov/main/www/popclock.html

[6] US Census Fact Finder, tinyurl.com/census-factfinder-18-and-over

[7] International Telecommunications Union (ITU), "Measuring the Information Society," www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf at PDF page 106.

[8] Economy at a Glance, www.bls.gov/eag/eag.us.htm

[9] Billion Dollar U.S. Weather Disasters, 1980-2009, http://www.infoplease.com/ipa/A0882823.html.

[10] MAAWG Email Metrics Program: The Network Operators Perspective, Report #12, Third and Fourth Quarter 2009 (issued March 2010), www.maawg.org/sites/maawg/files/news/MAAWG_2009-Q3Q4_Metrics_Report_12.pdf

[11] If we use the estimate that 90% of all email is unwanted and 10% is legitimate, that implies a 9:1 ratio of server and network capacity for unwanted email vs. legitimate email. The MAAWG estimates are intentionally very conservative with respect to spam levels. Other estimates have put the fraction of unwanted email as shockingly high as 97%; see for example, "Spam overwhelms e-mail messages," http://news.bbc.co.uk/2/hi/technology/7988579.stm. If the 97% Microsoft estimate mentioned in that BBC report holds broadly, ISPs and Enterprise IT shops would effectively be buying 32.3 servers (97/3) just to handle spam for every server they actually need to accommodate legitimate customer traffic.

[12] "Cybersecurity, Innovation and the Internet Economy" at pps. 44219-44220.

[13] "The Security of End User PCs -- An Empirical Analysis," Stefan Frei, Secunia, security.internet2.edu/ddcsw2/docs/sfrei.pdf

[14] "National Survey: Online Safety is a Personal Priority for Americans," August 10th, 2010, http://staysafeonline.mediaroom.com/index.php?s=43&item=62

[15] www.pcisecuritystandards.org/security_standards/pci_dss.shtml

[16] Consider statistics about the nature of what is being spammed, such as "During the first half of 2010, pharmacy spam accounted for the bulk of unsolicited messages sent worldwide," see http://news.bitdefender.com/NW1650-en--BitDefender-Malware-and-Spam-Report-Finds-E-Threats-Exploiting-Web-2.0-Platforms.html and the chart, "Percentage of Affiliate Brands In Spam," http://labs.m86security.com/2010/05/canadian-pharmacy-no-longer-king/ showing over 80% of all spam as associated with the "Canadian RX Drugs," "Canadian Pharmacy," "Dr Maxman," and "Online Pharmacy" brand pharmaceutical affiliate programs.

It is true that in some cases spammers are dropping pay-per-install malware without the end-user's consent and other spammers may have wholly non-monetary motivations (e.g., they might hypothetically be targeting politically or militarily sensitive intelligence targets), but we believe those exceptions are comparatively uncommon relative to mainstream affiliate program spammers.

[17] Guidelines on Electronic Mail Security, NIST Report SP800-45v2, http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf , page 6-5.

[18] "CBL Breakdown by Country, Highest 200 by Count," September 4th, 2010, cbl.abuseat.org/country.html

Geolocation of IP addresses listed on the CBL is described on that page as being done with a non-disclosed proprietary database; it is not believed to be based on domain names or other indicia which may be misleading for geolocation purposes.

[19] The BRIC countries are Brazil, Russian, India and China, see www.en.wikipedia.org/wiki/BRIC (for those who may have noticed that China did not make the top eight countries listed above, they were ranked 12th with 199,807 compromised hosts, a substantial improvement from where they were ranked at one time)

[20] For example, the Dell Small Business website is offering mini desktop computers (the Dell Inspiron Zino HD) starting at less than $250 at the time this was written. For comparison, Best Buy's Geek Squad virus and software removal (diagnose and repair) runs $149.99 online, $199.99 in store, and $299.99 in home/in office (see http://www.geeksquad.com/services/computer/service.aspx?id=2887) Thus, at least for old or basic computers, it may literally be more cost effective to replace them rather than trying to repair them.

[21] "We Need a Cyber CDC or Cyber World Health Organization," darkwing.uoregon.edu/~joe/ecrime-summit/ecrime-summit.ppt (or .pdf), Anti-Phishing Working Group (APWG) Counter E-Crime Summit, San Francisco, May 31, 2007.

[22] "Focus on Secrecy Could Hamper Pentagon's Cybersecurity Plans," August 30, 2010 http://threatpost.com/en_us/blogs/focus-secrecy-could-hamper-pentagons-cybersecurity-plans-083010

[23] See for example, "Can I obtain a security clearance on my own?" in http://www.clearancejobs.com/security_clearance_faq.pdf

[24] http://amada.abuse.ch/blocklist.php

[25] http://www.blade-defender.org/eval-lab/

[26] http://support.clean-mx.de/clean-mx/viruses.php

[27] http://www.malwaredomains.com/

[28] http://hosts-file.net/rss.asp

[29] http://malc0de.com/database/

[30] http://www.malware.com.br/lists.shtml

[31] http://mdl.paretologic.com/

[32] http://www.threatlog.com/

[33] See, for example, "Firefox Phishing and Malware Protection, www.mozilla.com/en-US/firefox/phishing-protection/, "Microsoft's Smart Screen Filter," www.microsoft.com/security/filters/smartscreen.aspx, "Opera Fraud and Malware Protection," http://help.opera.com/Mac/10.60/en/fraudprotection.html, and "McAfee Site Advisor," www.siteadvisor.com/.

[34] An example of a filtered DNS service is www.opendns.com. (OpenDNS offers protection from malware sites as part of their for-fee OpenDNS Enterprise product.)

[35] Reviews of some anti-malware Web gateways can be found at "Anti-Malware Gateways Group Test," www.scmagazineus.com/anti-malware-gateways/grouptest/209/.

[36] For a discussion of fast flux, including double flux, see "SSAC Advisory on Fast Flux Hosting and DNS," www.icann.org/en/committees/security/sac025.pdf.

[37] See RFC2775, "Internet Transparency," http://tools.ietf.org/html/rfc2775 and RFC4924, "Reflections on Internet Transparency," http://tools.ietf.org/html/rfc4924

[38] Spamhaus, www.spamhaus.org

[39] "Comments on the National Strategy for Trusted Identities in Cyberspace, MAAWG, July 19th, 2010, www.maawg.org/system/files/MAAWG_Comments_NSTIC_Trusted_Identities.pdf

[40] "Cybersecurity, Innovation and the Internet Economy" at pp. 44221.

[41] "Legal Attaché Offices," www.fbi.gov/contact/legat/legat.htm

[42] "Council of Europe Convention on Cybercrime Frequently Asked Questions and Answers," United States Department of Justice Computer Crime & Intellectual Property Section, www.justice.gov/criminal/cybercrime/COEFAQs.htm

[43] By way of example, higher education's nationwide research and education backbone network, Internet2, routinely encourages research *about* the network as well as research *over* the network. At the same time, Internet2 works diligently to carefully protect the privacy of its users' network traffic by appropriately anonymizing Netflow and other data before releasing it for researcher use. Unfortunately, there are few if any comparable sources for network research data from the commodity Internet. This lack of data directly and continually inhibits data-driven cybersecurity research and development outside the proprietary network operator community.

[44] "A Roadmap for Cybersecurity Research," November 2009, www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[45] "X Prize Foundation," http://www.xprize.org/

[46] "Cybersecurity, Innovation and the Internet Economy" at pp. 44222.

[47] "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," http://tools.ietf.org/html/rfc2827

[48] An ASN, or Autonomous System Number, is usually technically defined as a number assigned to a group of network addresses, managed by a particular network operator, sharing a common routing policy. Most ISPs, large corporations, and university networks have an ASN. For example, Google uses AS15169, Sprint uses AS1239, Intel uses AS4983, the University of California at Berkeley uses AS25 and so on. Some large networks with particularly complex routing policies may have more than one ASN; others, with simple routing policies and only a single upstream network provider, may have none (their network blocks are just announced using their upstream provider's ASN). Bottom line, in general, think of an ASN as a number that "maps to" or represents a particular provider or network. As such, it is a useful way to aggregate and sort IP addresses into useful chunks, even though its initial purpose (and continued most important usage) is in conjunction with BGP4 for inter-AS routing of network traffic. For more information, see "ASNs (Autonomous System Numbers)," www.uoregon.edu/~joe/one-pager-asn.pdf

[49] 24.2% of autonomous systems allow spoofed traffic as of Sunday September 5th, 2010. See "Spoofer Project: State of IP Spoofing," http://spoofer.csail.mit.edu/summary.php

[50] Botted hosts are malware infected end-user computers which are organized into botnets and controlled by a botmaster for purposes such as sending spam, conducting distributed denial of service (DdoS) attacks, click fraud, distributed scanning, etc. The Honeynet Project has an excellent introduction to bots and botnets at "Know Your Enemy: Tracking Botnets," 08/10/2008, www.honeynet.org/papers/bots/

[51] Whois is a distributed online database providing information about the users of Internet name and number resources such as IP addresses, domain names, autonomous system numbers, etc. For more information, see "The Whois Protocol," RFC3912, www.ietf.org/rfc/rfc3912.txt

[52] "Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information," developed by NORC at the University of Chicago for ICANN, 17 January 2010, www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

[53] "Whois Data Cleanup," www.arin.net/resources/request/whois_cleanup.html