To: National Institute of Standards and Technology (NIST)
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)
Date: April 8, 2013
Subject: Response to Request for Information: Framework for Reducing Cyber Risks to Critical infrastructure (http://www.nist.gov/itl/upload/rfi_02_12_13.pdf)

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is a global nonprofit organization founded to develop effective models to combat online threats such as botnets, phishing, malware, spam and denial-of-service attacks that can cause great harm to individuals, organizations and national economies. Representing more than one billion mailboxes, M3AAWG is the largest global organization developing cross-sector approaches to protecting users and network infrastructure.

Our members include technical experts, researchers and policy specialists from a broad base of network operators and from key technology providers, academia, government and volume messaging sender organizations. The multidisciplinary approach at M3AAWG (www.m3aawg.org) includes the development of industry best practices, education, technical statements on public policy and legislation, and the facilitation of global collaboration.

We appreciate the opportunity to respond to the NIST Request for Information on the Framework for Reducing Cyber Risks to Critical Infrastructure. We also are looking forward to participating in future discussions on these topics and to sharing our expertise with the agency. In these comments, we will address Questions 7 and 12, starting with the latter as way of introduction.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

No organizational entity, government or business is an island. The cybersecurity problem is best addressed today by aggregating, analyzing and sharing industry-wide threat data and building collective defense systems based on good information. International and standards bodies are a critical resource because they are extremely effective at driving the necessary collaboration, technology development and education that is needed to protect the ecosystem, and have, in fact, been shown to be the most efficient channel for immediate, responsive action.

Industry is leading the fight against today's cybercrime, which is still chiefly motivated by financial gains. The defense from online threats such as malware, socially engineered attacks, botnets and hijackings is very similar to those needed for broader protection against critical infrastructure. The industry's efforts over the last decade in this area have resulted in prolific domain-specific technology expertise and the creation of organizations, such as M3AAWG, as a channel for an integrated, rapid response to new and evolving threats. Rather than reinvent the wheel, the U.S. government should utilize such organizations and leverage the forward momentum that these organizations have amassed.

International organizations also provide opportunities for educating the industry and developing the necessary best practices to protect the global ecosystem. Like many of our partner organizations around the world, M³AAWG has undertaken this work for almost ten years and we have made real and positive gains.

The voluntary industry collaboration and best practices fostered by M³AAWG have proven to be a powerful and successful strategy in establishing online security. M³AAWG was formed in 2004 to fight spam and its associated problems at a time when email, one of the Internet's two "killer apps," was at risk of collapse. Today email is in a managed state of health: While M³AAWG members report that about 80% of current email traffic is abusive spam, they also are able to prevent over 99% of this overwhelming volume of spam from reaching end-users mailboxes.

This is due in large part because M³AAWG has become a trusted forum where the industry, government and academia can confidentially and securely work together. The organization is now applying its collaborative talents to developing actionable strategies impacting current and emerging security challenges in the areas of bots, malware and mobile.

As a technology-focused, non-political working body, M³AAWG has become a vital industry resource with a proven history of facilitating relationships and producing global best practices to effectively combat threats. Our cooperative approach is adaptable to the needs of diverse network environments and we make impartial, technical expertise available to industry and government agencies.

Our broad based membership includes leading ISPs, email providers, mobile network providers, social networking companies, public policy advisors, academic researchers, anti-abuse vendors and volume senders. We have reciprocal partnerships with the Internet Society (ISOC), the London Action Plan (LAP) and many other like-minded global Internet organizations. The M³AAWG Board includes AT&T, Comcast, Facebook, France Telecom, Google, PayPal, Symantec, Time Warner Cable and Yahoo! among others. A complete member roster is available at http://www.maawg.org/about/roster.

This cooperative approach has led M³AAWG to become a safe haven for driving security innovation and for the cross-sector collaboration necessary to combat abuse and online threats:

- The safe, confidential environment within the organization allows the various shareholders in the Internet ecosystem from all sectors to share the vital information necessary to stop online threats.
- The M³AAWG Email Metrics Report, produced since 2007, is the only spam report generated with data aggregated directly from network operators. As bots have become a major threat, we are extending this program and developing the first global network operator metrics on bots.
- M³AAWG Chairman Emeritus Michael O'Reirdan chaired the U.S. FCC committee that produced the first voluntary code outlining how network operators can work against bots and malware, the Anti-Bot Code of Conduct for ISPs (ABCs for ISPs). The CSRIC working group also involved other M³AAWG members.
- We developed the comprehensive Best Practices to Address Online and Mobile Threats with the London Action Plan (LAP) and submitted it to the Organisation for Economic Co-operation and Development (OECD). M³AAWG also worked with the OECD to produce its initial anti-spam tool kit.
- As India became a leading source of spam and other abusive messages, M³AAWG responded by creating an Indian chapter to spread the mitigation practice and methods. M³AAWG seeded this effort with a workshop in India on "Fighting Spam and Bots" attended by influential government and industry representatives preceding the EastWest Institute's global cybersecurity summit. In January

2013, we hosted a second meeting. The workshop presentations and documents are at www.m3aawg.org/india.

- The EastWest Institute selected M³AAWG to announce the first collaborative anti-spam effort between China and the United States, and M³AAWG has taken on the task of continuing that work.
- We host 300 to 500 security experts at our working meetings three times a year, including an annual European meeting, to collaborate on global anti-abuse issues. Keynotes and expert speakers have included U.S. ITU Ambassador Phil Verveer, FTC Consumer Protection Bureau Director David Vladeck, European Commission cybercrime official Radomir Jansky, DNS creator Paul Mockapetris, and officials from ICANN, IETF and Industry Canada, among others. We have hosted the GSMA Security Group and other mobile associations at our meetings.
- Concerned government entities are M³AAWG members and participate in the organization, including the U.S. Senate. In addition, several international anti-abuse and industry groups are members, including CAUCE; eco-Association of the German Internet Industry; ISC (Internet Systems Consortium); International Computer Science Institute (ICSI); .SE, the Internet Infrastructure Foundation; NCTA (National Cable & Telecommunications Association); Spamhaus; Shadowserver; and SURBL.
- We also produce expert training videos available to the industry on cutting-edge issues, such as assisting ISPs in identifying bots and strengthening their networks against malware, IPv6, the anti-abuse standards DMARC and DKIM, and other topics.

Having partnered with the U.S. government through the CSRIC working group and other activities, we are ready and eager to continue to collaborate in the cybersecurity fight.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

M³AAWG and its peer organizations have developed a diverse and important volume of best practices that address essential issues. Here too, the U.S. government should leverage existing work rather than investing valuable resources in reinventing what already exists.

M³AAWG best practices are developed through the collective experience of our members and technical advisors, representing a broad range of expertise that is not generally available to government agencies. These documents share our members' proven security experience with the Internet community, developing countries, and both large and small companies.

Overall, M³AAWG has developed 24 best practices and papers outlining procedures for network operators, senders and other industry entities. A few pertinent documents:

- M³AAWG Managing Port 25 (Dec. 2005)
  As many as 80% of all spam messages, much of it carrying concealed malware and bots, passes through "zombie" personal computers without the knowledge or authorization of their owners. Requiring authentication and aggregating email transmission traffic through SMTP relays addresses this issue.
- RFC 6561, "Remediation of Bots in ISP Networks" (March 2012)
  M³AAWG published the first best practices for mitigating bot infections in residential networks in July 2009. These are now incorporated into the 2012 IETF document.

- M³AAWG Best Practices for the Use of a Walled Garden (Oct. 2007)
  This document outlines practices ISPs can use to stop their network from being used for abusive purposes by making end-users aware of unwanted malware residing on their personal computers.
- M³AAWG BCP for Mitigating Abuse of Web Messaging Systems (Aug. 2010)
  As spam filters have improved at blocking direct connections from spammers, cyber criminals increasingly are turning to Web-based messaging systems to transmit their content. This document describes techniques to prevent or mitigate these attacks, detailing the best practices for protecting Web-based systems.
- M³AAWG Complaint Feedback Loop BCP (Aug. 2010)
  Complaint Feedback Loops have existed for more than a decade, resulting in many de facto standards and best practices. This document clarifies the ways that both providers and consumers of these feedback mechanisms can use the feedback, describing some common industry best practices. IETF RFC 6449, authored by a M³AAWG member, also outlines this process.
- M³AAWG Overview of DNS Security - Port 53 Protection (June 2010)
  ISPs are uniquely positioned to protect their subscribers by carefully managing access to network resources. The Domain Name System (DNS) is central to the proper functioning of virtually every Internet Protocol (IP)-based communication in every network across the Internet. Consequently, managing access to the DNS is an essential part of the overall security posture of every subscriber.
- M³AAWG Sender Best Communications Practices
  M³AAWG published the first senders best practices developed through the cooperative efforts of network operators and volume email senders.
- M³AAWG Position on Email Appending
  M³AAWG position against email appending has received wide industry support.

These best practices have worked well to reduce spam, a major carrier of bots and malware, and are widely adopted throughout the industry. The depth of knowledge and expertise of our membership allows us to develop new best practices as needs arise and we are currently working on other projects. The trusted forum at M³AAWG is an extremely valuable resource for identifying vital areas of concern and developing a broad, industry-wide consensus to address the issue.

We look forward to participating in the continued dialogue as NIST develops the Framework and to being of service to the agency. Please address any questions or requests for additional information to Jerry Upton, M³AAWG Executive Director at jerry.upton@m3aawg.org

Yours truly,
s/s
Jerry Upton
Executive Director, M³AAWG
jerry.upton@m3aawg.org