To: Mr. Andrew Harris, U.S. State Department (via email at cwg.internet@state.gov)
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)
Date: January 9, 2014
Subject: M^{3}AAWG Response to Stakeholder Input on the Role of Governments,
ITU-CWG on Internet-related Public Policy Issues

The Messaging, Malware and Mobile Anti-Abuse Working Group is where the industry comes together to work against bots, malware, spam, viruses, denial-of-service attacks and other online exploitation. M^{3}AAWG (www.M3AAWG.org) is a global nonprofit representing more than one billion mailboxes from some of the largest network operators worldwide; we are 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, key technology providers, academia, government and volume messaging sender organizations. The multidisciplinary approach at M^{3}AAWG 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 comment on the United States' submission to the CWG-Internet. We have briefly described our relevant work in the selected public policy sections in the state department's provided chart. For a more detailed understanding of these issues, we direct you to our response to the CWG-Internet Request for Online Consultation-Combatting Spam of July 31, 2013, which is also attached.

In our July 2013 response, we indicated that based on our ten years of global experience in reducing spam levels, we have found that the most important elements in addressing Internet development and anti-abuse efforts are:

1) the widespread adoption of proven best practices based on shared industry expertise and

2) industry collaboration in an environment of mutual trust and open dialogue

To this end, M^{3}AAWG has worked hard to create a vetted environment that supports an ongoing industry dialogue addressing current and emerging issues, including organizing three, four-day meetings each year. We have generated 23 best practices and white papers with proven techniques to reduce abuse and have submitted 30 memos to various organizations, such as ICANN, ARIN and governmental agencies, commenting on technical issues relating to regulatory issues.

Our anti-abuse efforts include:

- Publishing the comprehensive "Best Practices to Address Online and Mobile Threats" developed with the London Action Plan and presented to the OECD (Organisation for Economic Co-Development)
- Issuing best practices on managing port 25 that have significantly contributed to reducing spam
- Developing best practices to help ISPs mitigate malware on subscribers' systems that became the basis for the IETF's RFC 6561
- Developing joint anti-abuse best practices with the OECD and the Anti-Phishing Working Group
- Publishing the only metrics reports of abusive email from data provided directly by network operators
- Recently establishing the M^3 Anti-Abuse Foundation, a new nonprofit to provide anti-abuse training and educational resources to regions with developing Internet infrastructure

If needed, more information on our organization and activities can be found at www.m3aawg.org:

- A complete member listing is at http://www.m3aawg.org/about/roster/
- A list of published documents can be found at http://www.m3aawg.org/published-documents.
- M3AAWG public policy comments are at http://www.m3aawg.org/activities/published-comments
- M3AAWG Email Metrics Reports can be accessed at http://www.m3aawg.org/email_metrics_report
- Training videos are available at http://www.m3aawg.org/activities/maawg-training-series-videos with additional video on YouTube at https://www.youtube.com/user/MAAWG/videos
- Upcoming meeting dates and locations are at http://www.m3aawg.org/events/upcoming_meetings

We will be glad to respond to any questions. Please address any inquiries about our work to me, M3AAWG Executive Director Jerry Upton, at jerry.upton@m3aawg.org.

Sincerely,
Jerry Upton, M3AAWG Executive Director
Jerry.Upton@m3aawg.org

Public Policy Issues	Relevant ITU Mandate (per Resolution 1305)	Role of Governments	Role of ITU	Existing Venues to addressing issues
Multilingualization of the Internet Including Internationalized (multilingual) Domain Names	**PP. Resolution 133** (Rev. Antalya, 2006) **WTSA Resolution 48** (Rev. Johannesburg, 2008) **WTDC Programme 3** (Rev. Doha, 2006)			
International Internet Connectivity	**ITU-D Study Group 1, Question 12**-2/1 **ITU-T Study Group 3** (**Recommendation D.50**)			
International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses	**PP. Resolutions 101**, **102** (Rev. Antalya, 2006) **WTSA Resolutions 47**, **49**, **64**, **69**, **75** (Rev. Johannesburg, 2008) **Resolution 1282** (Mod. 2008) **Lead Facilitator of WSIS AL C6 (Tunis 2005)**			M^{3}AAWG has submitted 30 comments responding to various policy organizations over the last 10 years, including responses to ICANN, ARIN, PNIC/LACNIC/AFRINIC and various governmental agencies. See the complete list at www.http://www.m3aawg.org/activities/published-comments
The security, safety, continuity, sustainability, and robustness of the Internet	**PP. Resolutions 102**, **130** (Rev. Antalya, 2006) **WTDC Resolution 45**, **Programme 3** (Rev. Doha, 2006), **WTSA Resolutions 50**, **52** (Rev. Johannesburg 2008) **ITU-T Study Group 17**, **ITU-D Study Group 1** **PP. Resolution 71 – Strategic Goal 4** (Rev. Antalya, 2006)			M^{3}AAWG work in this area is too extensive to list here with 23 relevant best practices published to date, which can be found at http://www.maawg.org/published-documents. Some highlights: • In 2012, we issued the Best Practices to Address Online and Mobile Threats together with the London Action Plan. • We have also cooperated with the OECD on anti-spam best practices and presented to them on anti-spam and anti-malware issues. • We developed the first best practices to help ISPs mitigate malware; became the basis of RFC 6561. • We issue the only reports of abusive email with data provided directly from

				network operators. • We are developing the first network operator-based bot metrics. • Our best practices on managing port 25 has led to significant reduction in spam and abusive email. • We issued the first senders best practices developed cooperatively between ESPs and network operators. • Our chairman chaired the U.S. CSRIC Working Group 7 when it developed the first U.S. Anti-Bot Code for ISPs, which also involved many of our members, and we host a page with the Code on our site. • We have a cooperative liaison relationship with the IETF and have hosted presentations by the ICANN safety and security team to educate Internet professionals. • We have created a comprehensive library of training videos to educate professionals on how to operate more safely, including leading experts detailing how ISPs can identify and clean malware from their subscriber systems, videos on implementing accepted standards such as DKIM, and a course on IPv6 implementation. • Our work provides a platform for data-sharing in support of anti-botnet initiatives such as Botfree, a site to inform consumers about bots with information on how to clean their systems that is a service of eco, the Association of the German Internet Industry, and the Advanced Cyber Defense Center that is fostering an extensive sharing of information across European Union Member States to improve the early detection of botnets and is building a network of cyber defense centers.

Combating Cybercrime	**Lead Facilitator of WSIS AL C5 (Tunis 2005)** **WTDC Programme 3** (Rev. Doha, 2006) **PP. Resolution 71 – Strategic Goal 4** (Rev. Antalya, 2006) **ITU-D Study Group 1**			• M^{3}AAWG has published best practices jointly with the Anti-Phishing Working Group (APWG) and LAP. • M^{3}AAWG has provided law enforcement training with LAP at M^{3}AAWG meetings. • We have provided training and working sessions on incident reporting and other related topics at M^{3}AAWG meetings. • M^{3}AAWG has new Special Interest Groups developing best practices and educating the industry on identity management and on hosting issues. • M^{3}AAWG has done abuse management, incident reporting and related training work in collaboration with APWG, CAUCE, LAP and the GSMA Security Group.
Dealing effectively with spam	**Lead Facilitator of WSIS AL C5 (Tunis 2005)** **PP. Resolution 130** (Rev. Antalya, 2006) **WTDC Programme 3**, **Resolution 45** (Rev. Doha, 2006) **WTSA 50**, **52** (Rev. Johannesburg 2008)			See the M^{3}AAWG response to the ITU CWG-Internet, July 2013 for details.
Issues pertaining to the use and misuse of the Internet	**Lead Facilitator of WSIS AL C5 (Tunis 2005)** **Resolution 1282** (Mod. 2008) **WTDC Programme 3** (Rev. Doha, 2006) **PP. Resolution 130** (Rev. Antalya, 2006) **WTSA Resolutions 50**, **52** (Rev. Johannesburg 2008)			• M^{3}AAWG has collaborated and presented to the OECD on spam and malware issues. • We have developed joint industry educational meeting sessions on various law enforcement issues with LAP. • M^{3}AAWG has collaborated with the APWG to develop and share best practices. • We have co-hosted meetings with the GSMA Security Group.

Availability, affordability, reliability, and quality of service, especially in the developing world	**Lead Facilitator of WSIS AL C2 (Tunis 2005)** **Resolution 1282** (Mod. 2008)			
Contributing to capacity building for Internet governance in developing countries	**WTDC Resolutions 17**, **20** (Rev. Doha, 2006) **ITU-D Programme 3**, **ITU-D Programme 5**, **WTSA Resolutions 64** (Rev. Johannesburg 2008)			• M^{3}AAWG organized an initial anti-spam workshop in India at the invitation of the EastWest Institute and has followed up by hosting several Indian meetings to promote local industry collaboration. • M^{3}AAWG sent professionals to train local Internet professionals on anti-abuse techniques as part of ISOC workshops in Kenya and Argentina. • M^{3}AAWG has established the M3 Anti-Abuse Foundation (M^{3}AAF), a new non-profit to support training needs in countries with developing Internet infrastructure. (See www.m3aaf.org.)
Developmental aspects of the Internet	**WTDC Resolutions 17**, **20** (Rev. Doha, 2006) **WTSA Resolutions 64**, **75** (Rev. Johannesburg 2008) **PP. Resolutions 101**, **102**, **133** (Rev. Antalya, 2006)			
Respect for privacy and the protection of personal information and data	**PP. Resolution 130** (Rev. Antalya, 2006) **Lead Facilitator of WSIS AL C5 (Tunis 2005)** **Resolution 1282** (Mod. 2008) **PP. Resolution 71 – Strategic Goal 4** (Rev. Antalya, 2006)			• M^{3}AAWG has provided educational advice on the technical aspects of pending legislation and international policy. • We have provided identity management and other topical training.
Protecting children and young people from abuse and exploitation	**PP. Resolution 130** (Rev. Antalya, 2006) **Lead Facilitator of WSIS AL**			M^{3}AAWG has hosted educational speakers and keynotes to help inform ISPs and industry professionals on this issue and train personnel to deal with this problem.

	C5 (Tunis 2005) **PP. Resolution 71 – Strategic Goal 4** (Rev. Antalya, 2006) **Resolution 1282** (Mod. 2008) **ITU-D Programme 3**, **ITU-T Study Group 17**			

M^{3}AAWG
MESSAGING MALWARE MOBILE

To: ITU Council Working Group on International Internet–Related Public Policy Issues (CWG–Internet)
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)
Date: July 31, 2013
Subject: Response to CWG-Internet Request for Online Consultation-Combatting Spam

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) is a global nonprofit association founded to develop effective models to combat online threats such as spam, botnets, phishing, malware and denial-of-service attacks that can cause great harm to individuals, organizations and national economies. Representing more than one billion mailboxes, M^{3}AAWG 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 M^{3}AAWG (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 request from the ITU Council Working Group on International Internet–Related Public Policy Issues (CWG–Internet) for online consultations from all stakeholders. We will be focusing our remarks on the first issue:

- **Issue 1: Consultation on effectively countering and combatting spam**
  The Council Working Group on International Internet-Related Public Policy Issues invites all stakeholders to provide input on international public policy issues related to effectively countering and combatting spam.

While this topic is somewhat broad, we welcome the invitation to share our global experience in reducing spam levels and to explain the strategies that have proven most effective in almost ten years of working together against Internet abuse. M^{3}AAWG was formed as a working body 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.

In tackling the issue over the years, we have realized that despite the astoundingly higher volumes of spam today, our members have been able to prevent all but a relatively small percentage of this abusive email from being delivered to users' inboxes. This is documented in our quarterly M^{3}AAWG Email Metrics Reports[1] with data collected directly from global network operators aggregating the quantity of abusive mail identified and the percentage delivered to end-users. Email continues to thrive in a managed state of health in much of the world.

What has worked? The most powerful tools we have identified for expunging increasing volumes of spam from both established and growing networks has been 1) the widespread adoption of proven best practices based on shared industry expertise and 2) industry collaboration in an environment of mutual trust and open dialogue.

With this historical assessment, we respectfully submit to the ITU Council Working Group-Internet that there is an active and multi-stakeholder community, which has, collectively, been engaged on this issue for more than a

[1] Email Metrics Program: The Network Operators' Perspective with reporting beginning in April 2007. Reports are available at http://www.m3aawg.org/email_metrics_report

decade. M^{3}AAWG, especially, is widely recognized as the forum of choice for cooperation in a vendor-neutral, collegial and vetted environment on the technical issues necessary to protect service providers and end users.

However, M^{3}AAWG fully realizes that Internet service providers in emerging economies continue to face significant problems with Internet abuse, and so works to extend the best practices developed by its members to industry entities around the world by:

1. Making translations of many M^{3}AAWG best practice documents available in multiple languages, including all the official languages of the United Nations
2. Organizing and participating in outreach initiatives
3. Actively engaging with other relevant stakeholders around the world, across governments, industry and civil society

M^{3}AAWG looks forward to working closely with the ITU to promote the voluntary adoption of existing and future best practices and to encourage global cooperation on capacity building in emerging Internet economies.

To this end, M^{3}AAWG has worked over the years to foster a respected, vetted community for dialogue and information sharing – and has created the necessary meetings and infrastructure – allowing our members to privately share their experiences with effective anti-spam strategies and then distribute this distilled knowledge to the industry as best practices. We also have successfully partnered with other inter-governmental, industry and civil society organizations to bring specialized talents and resources to more effectively address rapidly morphing threats.

For example, M^{3}AAWG collaborated with the London Action Plan (LAP) last year in producing the "Best Practices to Address Online and Mobile Threats[2]," a comprehensive 52-page report outlining proven tactics against abuse. LAP is a highly respected network of organizations engaged in anti-spam and law enforcement; M^{3}AAWG shared its technical competency, collaborative knowledge and real-world experience. The resulting jointly authored report has been submitted to the OECD for consideration and implementation by both business and government entities. It contains the collective knowledge of experts from around the world on how to reduce online risks, augmented with forward-thinking recommendations to tackle emerging vulnerabilities, such as mobile text spam and Web abuse.

As spammers grow more sophisticated and emboldened, it has become increasingly difficult for an isolated and politicized world to keep pace with evolving threats. As stated in the M^{3}AAWG/LAP report, "... Spam is not just an email phenomenon. It continues to expand into various forms of new media. For example, mobile messaging and Voice over Internet Protocol (VoIP) spam are now extremely common, as are spam comments on social media, blogs and other websites…"[3] In confronting the complex malady of today's spammers, the technical specialists working with these issues every day have come to depend on the vetted channels available through industry associations to share their discoveries with the world in reports such as this one.

This approach is adaptable to the needs of both specific countries and network environments. Industry best practices and information sharing programs support anti-abuse efforts in both large and small companies, and in countries with both established and developing Internet infrastructure. M^{3}AAWG, like other industry associations, has engaged in numerous outreach programs that have also contributed to curtailing spam, including:

[2] "Best Practices to Address Online and Mobile Threats," Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) and London Acton Plan (LAP), October 2012, http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf

[3] Ibid, page 5

- Our port 25 management best practices have been widely adopted as an effective anti-spam strategy. M^{3}AAWG also issued the first best practices to help ISPs work with customers to mitigate bots and malware, which became the basis of the IETF's RFC 6561.
- Among the 25 best practices we have issued, M^{3}AAWG published the first senders best practices developed through the cooperative efforts of network operators and volume email senders, and the M^{3}AAWG position against email appending has received wide industry support.
- We have responded to 27 requests for comments outlining how the technical aspects of public policy would affect the industry's ability to identify and curtail spam, including responses to ICANN and other Internet governing bodies, and to both North American and European public policy agencies.
- We continue to partner with other organizations, including working with the OECD to produce its initial anti-spam tool kit. While serving as M^{3}AAWG co-chairman, Michael O'Reirdan chaired the U.S. FCC CSRIC 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[4] (ABCs for ISPs). The CSRIC committee also involved other M^{3}AAWG members.

International cooperation is essential to stopping abusive messaging. Industry associations like M^{3}AAWG provide a proven and vetted environment for the necessarily sensitive dialogue among global competitors and law enforcement.

- In India, M^{3}AAWG offered an anti-spam workshop at the request of the EastWest Institute (EWI) attended by influential industry representatives and we continue to host two additional meetings a year to facilitate Indian industry cooperation against spam. Information and related documents for the India Anti-Abuse Working Group are available at www.m3aawg.org/india.
- The East West Institute selected M^{3}AAWG to announce the first collaborative anti-spam effort between industry stakeholders in China and the United States, and M^{3}AAWG has taken on the task of continuing that work.
- We often host other organizations such as the LAP and the GSMA Security Group at our meetings. M^{3}AAWG meetings bring together 300 to 400 leading security professionals for confidential dialogue three times a year, including an annual European meeting. The meetings offer more than 30 training, educational and dialogue sessions and keynotes have included FTC Bureau of Consumer Protection Director David Vladeck, INTERPOL's Assistant Director Michael Moran, U.S. ITU Ambassador Phil Verveer, European Commission Justice Freedom and Security DG Radomir Jansky, DNS creator Paul Mockapetris, and officials from ICANN, IETF and Industry Canada, among others.
- We have produced pertinent training videos with recognized experts detailing malware mitigation techniques, anti-spam protocols and other anti-abuse tactics that are available to the general industry.
- We issue the only email metrics reports generated with anonymized and aggregated data sourced directly from network operators and are currently developing the first operators' bot metrics report.

[4] **Final Report: The Anti-Bot Code of Conduct for Internet Service Providers** (A Voluntary Code)**,** The Communications Security, Reliability and Interoperability Council Working Group 7, available at http://www.maawg.org/abcs-for-ISP-code.

- Many concerned government entities are members and participant in M^{3}AAWG dialogues, including the U.S. Senate's IT department, and other organizations such as CAUCE; eco, an association of German ISPs; ISC (Internet Systems Consortium); International Computer Science Institute (ICSI); .SE, the Internet Infrastructure Foundation; the Internet Society (ISOC); NCTA (National Cable & Telecommunications Association); Spamhaus; Shadowserver; and SURBL.

These and other efforts by various industry associations are considered by many security experts, public policy advisors and government entities to be among the most efficient programs for confronting spam and abuse.

We encourage the CWG-Internet to focus on promoting the voluntary adoption of existing best practices developed by impartial industry associations that represent the best thinking of experienced technical experts. Promoting and supporting industry best practices developed by experts is the best use of resources versus working to create new procedures and incurring the time delays associated with replicating existing work.

Speaking for M^{3}AAWG, you can find all our best practices, training videos and other materials on our website at www.m3aawg.org. I will be glad to respond to any questions or provide more information. You can also address any inquiries about our work at M^{3}AAWG to me, M^{3}AAWG Executive Director Jerry Upton at jerry.upton@m3aawg.org.

Sincerely,
Jerry Upton, M^{3}AAWG Executive Director
Jerry.Upton@m3aawg.org