Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) Comments on Request for Information on the Development of an Artificial Intelligence (AI) Action Plan

Published document: 2025-02305 (90 FR 9088)

Introduction

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) appreciates this opportunity to comment on the Request for Information on the Development of an Artificial Intelligence (AI) Action Plan. We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet.

M^{3}AAWG is a technology-neutral global industry association. With more than 200 members worldwide, we are the largest such organization in the online community. We bring together stakeholders in a confidential trusted forum to develop best practices and cooperative approaches for fighting online abuse. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. M^{3}AAWG works to fight online abuse caused by botnets, malware, spam, phishing, ransomware, viruses, denial of service (DoS) attacks, and other forms of online exploitation.

We appreciate the opportunity to submit comments to the Office of Science and Technology Policy (OSTP) regarding high-priority AI policy actions for consideration. While many potential policy actions could be included in a new AI Action Plan, we would like to focus on three key elements: AI security and AI for security; AI standards and best practices; and collaboration between industry, government and other stakeholders.

AI and Security: Securing AI and Using AI for Security

As an anti-abuse and security organization, we would like to underscore the importance of AI and security in three intersecting, key dimensions:

- Securing AI systems to prevent abuse of these systems by cybercriminals and creating opportunities for the adoption of secure AI;
- Using AI to secure computer systems, e.g., by automating and improving security controls; and
- Securing critical AI assets, such as personally identifiable or sensitive information used to train AI models, from being exfiltrated and abused to the detriment of individuals, businesses, and national security.

Therefore, M^{3}AAWG would like OSTP to consider the following recommendations:

- We urge that future and existing federal programs support stakeholder efforts in monitoring and managing AI system risks. While much progress has been made by NIST, CISA, and other organizations, supporting further work, especially on how to practically implement mitigations and how to prevent misuse of AI systems (e.g., deepfakes), would be of great use. In particular, we urge support for:

  - Research and development initiatives that provide guidance on how to develop AI systems that can adapt to evolving cyber threats. This work can build on existing frameworks like the NIST AI Risk Management Framework and multiple ongoing efforts of NIST to further develop AI (security) standards.
  - Federal research initiatives and incentives for the private sector to create risk-based models and tools for secure AI development lifecycles, following a philosophy of security and privacy by design.
  - Programs that support the ecosystem of open-source tools that help build security and privacy in AI applications from the get-go, rather than being "bolted on" at a later stage.
  - Federal initiatives to support training and education programs for public sector agencies to evaluate risk from and to AI systems within critical government cybersecurity infrastructure. AI innovation and risk management will also need a trained workforce.
- AI is a powerful tool for detecting and mitigating online threats such as spam, phishing, and malware. We would like to underline the importance of support for R&D programs through public-private partnerships that develop AI applications focused on cybersecurity enablement and abuse prevention.

AI Standards and Best Practices

To achieve greater security and privacy, we recommend further investment into relevant standards, best practices, and benchmarks that support AI developers, service providers, and users in securing AI systems and the AI lifecycle.

- Establishing and harmonizing clear baseline standards is of central importance. Clear standards regarding definitions, architectures, and product profiles will ensure clarity, understanding, and transparency in the marketplace.
  - All stakeholders (developers, service providers, users, etc.) must be able to understand supply chains, products, and systems to manage risks appropriately and to secure their systems.
  - A growing number of organizations rely on external AI service providers and depend on transparency to secure their systems.
  - AI supply chains are often inherently complex and require various third parties and components such as externally acquired foundational models and training data, various AI service and infrastructure providers, and external developers.
- Thus, we encourage the creation of risk profiles, standards, and best practices for foundation model developers, deployers, and users, especially for high-risk use cases. We also encourage supporting the

development of public datasets that can be used as benchmarks for evaluating AI models across different use cases.

- Focused support of best practice development on how to address AI abuse by cybercriminals and other adversaries is desperately needed. Therefore, we urge deep engagement with security and AI experts in government (e.g., CISA, NIST) with anti-abuse organizations, including, but not limited to, the Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG).
- NIST and other relevant organizations should develop further insights and technical standards on how to create secure, reliable, and effective AI systems with significant industry input, especially when it comes to combating online abuse and securing networks and (AI) systems from adversaries.
  - We note that anti-abuse and anti-fraud are distinct from, if related to, safety, security, privacy and reliability; best practices must be established and followed to protect against the negative impact of powerful AI tools being misused by criminals, causing financial and other harm to people and the nation.

Collaboration Between Industry and Government / Stakeholders

To address the above-mentioned concerns, we underline the importance of strong collaboration between different stakeholders, not only when it comes to developing standards and engineering approaches but also when sharing operational information among government, private, and community actors. Therefore, we recommend that OSTP encourage and enable:

- Partnerships between government agencies, industry groups like M^{3}AAWG, and other global AI ecosystem stakeholders to share knowledge and resources for AI development and deployment.
- Information sharing between relevant AI stakeholders to identify threats and coordinate mitigation efforts for the protection of individuals, the economy, and the nation.

Conclusion

We appreciate the opportunity to submit these comments and welcome further opportunities to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director
Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG)
P.O. Box 9125, Brea, CA 92822
comments@m3aawg.org

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.