Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) on NIST AI 100-4, Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency

Consultation reference: NIST AI 100-4, Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) appreciates the opportunity to submit comments in response to the above-referenced consultation. M^{3}AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community in a confidential yet open forum, developing best practices and cooperative approaches for fighting online abuse.

Synthetic content is already a concern in areas such as profit-oriented cybercrime, fake news, and election interference. It therefore represents a risk to national security as a whole. M^{3}AAWG welcomes the opportunity to comment on the current version of NIST AI 100-4 from our perspective as security and anti-abuse specialists.

1. M^{3}AAWG fully supports the primary goal of this document and acknowledges the immense amount of work that went into its content. However, the document mainly discusses stop-gap measures that cannot appropriately mitigate pertinent risk. In all likelihood, this is due to the fact that existing protocols, approaches, and technologies are not (yet) sufficiently capable in addressing the risks created by the abuse of synthetic content. A new or evolved approach may have to be developed to address this issue. In the meantime, it may be possible to cryptographically assure the integrity of metadata and content using the same mechanism for both, ensuring that both are sufficiently protected.

2. The process proposed in section 6 figure 2 (p. 43) would be improved by changing the order and approach. Specifically, an overall assessment of the system and approach appears to happen as the last of many steps. The process should begin with an assessment of the overall planned system, considering system objectives, planned data and system architecture, and relevant risks. Not considering such concerns from the outset could lead to suboptimal outcomes. For example, a late consideration of high-level issues might not lead to sufficient changes due to sunk costs. We thus propose

to start the process with an initial overall impact and risk assessment, which is then updated and considered during the following assessment steps.

We appreciate the opportunity to submit these comments, and we 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
comments@m3aawg.org
P.O. Box 9125 Brea, CA 92822