To: ICANN
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
Date: January 26, 2018
Subject: M³AAWG Comments on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation

M³AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, appreciates this opportunity to comment on the Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation (https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf .) We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet, including the domain name ecosystem.

M³AAWG recognizes ICANN's work toward developing the proposed interim compliance models for continuing the discussion with the community and M³AAWG expresses its interest in, and support for, Model 2B. For context, please refer to the section "User Type: DNS Abuse/Security Researcher" within the document "gTLD Registration Dataflow Matrix and Information" (https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-whois-06nov17-en.pdf).

M³AAWG agrees that Model 2B provides the minimum data that registries and registrars would be required to publish in public registration directory systems[1], absent express consent from the registrants as required by the GDPR. While having more data fields displayed in the public WHOIS certainly facilitates correlational analysis, which allows for more effective identification and mitigation of threats and in turn for better user protection worldwide, M³AAWG understands and respects the GDPR imperative and the inevitable removal of certain data fields from the public WHOIS output.

M³AAWG notes that no data fields should be removed from the minimum data proposed by Model 2B, as doing so would hinder the effectiveness of the work performed by the anti-abuse community. The harm to users will likely increase if criminal activity can no longer be detected due to the lack of the necessary information in the domain name and WHOIS ecosystem.

M³AAWG agrees with the registrant opt-in requirement for publication of the Registrant Name. Regarding the retention of data during one year beyond the life of the registration, M³AAWG would prefer this time period be extended to two years, with the clarification that the two years should be counted only after the domain names are deleted at the registry level, not simply when they expire at the registrar.

In relation to the formal accreditation or certification program, M³AAWG notes that Model 2B lacks mention of anti-abuse and threat researchers, who must be allowed to become accredited or certified. This group requires access to non-public registration data in order to detect threats, new attack vectors and understand trends aimed at protecting users and the internet as a whole.

[1] This includes name of the Registered Name, information about the primary and secondary name servers for the Registered Name, information about the Registrar, the original creation date of the registration, the expiration date of the registration, the email address of the administrative contact for the Registered Name, and the email address of the technical contact for the Registered Name.

Of course, a key element of any accreditation or certification program is the criteria that will define the qualifications or conditions that applicants must meet in order to become certified or accredited. M³AAWG will be available to provide any and all appropriate feedback required to establish a transparent accreditation program for all involved parties.

Should the accreditation or certification program not be ready by May of 2018, as an interim solution, aside from law enforcement and intellectual property lawyers, the following parties should be allowed access to the non-public registration data:

- Incident response teams as listed by the Forum of Incident Response and Security Teams (FIRST)
- Organizations or individuals who are members of the Anti-Phishing Working Group (APWG) and the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
- Members of internationally recognized associations like the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), the Association of Certified Fraud Examiners (ACFE), the Internet Security Alliance or the International Association of Privacy Professionals (IAPP)

Anti-abuse and threat research professionals must be able to continue to access the minimum public data provided by Model 2B. For the health and security of the internet, these same researchers must be allowed to access non-public data via an appropriate certification or accreditation program. Failure to allow these professionals to access this data will only result in higher abuse rates, more harm inflicted on users and more criminal impunity on a global scale.

Sincerely,
[SIGNATURE]
/s/
Jerry Upton, Executive Director

Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109
https://www.m3aawg.org