To: ICANN (Internet Corporation for Assigned Names and Numbers)
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)
Date: March 10, 2018
Subject: M3AAWG Comments on Proposed Interim Calzone Model 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 GDPR Compliance (the "Calzone Model," https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-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.

On January 26th, 2018, M3AAWG commented in support of Model 2B on the interim models proposed by ICANN. M3AAWG agrees that the proposed Calzone Model, a derivative of 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 or an alternative legal basis, as required by the GDPR.

M3AAWG understands and respects the GDPR imperative and the likely inevitable removal of certain data fields from the public WHOIS output. However, M3AAWG members have a specific interest in supporting ICANN's stated goal of preserving as much of the WHOIS directory as possible. The more data fields displayed in the public WHOIS, the more it facilitates correlation analysis, which allows for more effective identification and mitigation of threats and, in turn, serves the public interest with better user protection worldwide and continued security, stability and resiliency of the DNS as a global system.

In pursuit of that shared goal, we ask that the ICANN organization, the ICANN community and ICANN's Governmental Advisory Committee be made aware of our concerns regarding the following:

- The Calzone Model currently lacks mention of any process that will ensure continued access to the full WHOIS directory for security and threat researchers and anti-abuse personnel.
- These organizations and individuals (including many of our members) frequently leverage registration data in order to detect threats or new attack vectors and to understand trends aimed at protecting users and the internet as a whole.
- Law enforcement authorities, both civil and criminal, very often rely on data obtained by private sector researchers and security professionals. Defenses against many different types of threats are also very often erected by the private sector, thanks in large part to registration data that they obtain, correlate and analyze.
- The GDPR recognizes that personal data may be processed on one or more grounds other than consent:
    - Article 6(1)(b) provides that data may be processed if to do so is a natural consequence of a contract. Those who register domain names with their registrars do so under the terms of contracts, in part drafted to provide compliance with the terms of ICANN. The requirements under paragraph 3.18 of ICANN's 2013 Registrar Accreditation Agreement can reasonably be interpreted to enable access for the purposes of countering fraud, illegal activity and abuse.

[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.

- Article 6(1)(e) provides that data may be processed if doing so is in the public interest. The agents performing that processing may be a private or public authority. Clearly, M³AAWG members, as well as operational security professionals in general, who work to counter threats, abuse and illegal activity are doing so in the public interest. Public law enforcement and security agencies frequently rely on the work performed by our members, along with security practitioners not affiliated with M³AAWG, to inform their actions.
- Article 6(1)(f) of the GDPR allows for the legitimate interest of the data controllers to be considered grounds for processing, where those grounds are not overridden by the rights of the data subjects. In the case of the WHOIS data, the data subjects have all entered into commercial contracts for the provision of particular services on terms that will all include provision for action in the event of illegal use of the domain names. It cannot be a breach of those data subjects' rights to take steps aimed at assessing compliance with – and enforcing – those provisions.

- For these reasons, we strongly urge ICANN to ensure that the criteria that will define the qualifications or conditions that applicants must meet in order to access the full WHOIS information includes provisions for security and threat researchers and anti-abuse personnel. M³AAWG will be available as needed 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, it is essential to provide access until the program is ready. As an interim solution, in addition to 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) https://www.first.org/members/teams/
  - 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), and the Internet Security Alliance.

Anti-abuse, security and threat research professionals must be able to continue to access the minimum public data provided by the Calzone Model – without which a significant negative impact on the security and reliability of the DNS and the internet as a whole would result. For the health and security of the internet, these same researchers and anti-abuse practitioners 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. The European Union's General Data Protection Regulation does not require that any of this occur. The Internet Corporation for Assigned Names and Numbers should take steps to ensure that it does not either.

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