M3AAWG
MESSAGING MALWARE MOBILE

August 12, 2013
To: ICANN
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)
Date: 12 August 2013
Subject: Comments on the Expert Working Group Initial Report

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is a global nonprofit organization founded to develop effective models to combat online threats such as botnets, phishing, malware, spam and denial-of-service attacks that can cause great harm to both individuals and national economies. Representing more than one billion mailboxes, M3AAWG 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, and volume messaging sender organizations. The multidisciplinary approach at M3AAWG (www.m3aawg.org) includes the development of industry best practices, educational tools, technical statements on public policy and legislation, and the facilitation of global collaboration.

We appreciate the opportunity to comment on the EWG Initial Report. We commend ICANN's desire to make WHOIS data more accurate, and the service technically more consistent, but we have some concern about the treatment of privacy and proxy services, and grave concerns about the proposed gated access.

Based on examinations of gTLD zone files and other data, we have found that the vast majority of domain names registered in gTLDs are registered for commercial purposes. While we fully appreciate that natural persons have legitimate privacy rights that need protection, the current situation is that the majority of privacy and proxy-protected domains are clearly used for commercial purposes. Commercial registrants do not need privacy protection, and in fact, legitimate businesses should have no need to hide their identities from their current or potential customers. Many national TLD operators, such as CIRA in Canada and Nominet in the UK, have policies that allow as an exception private registration for natural persons using their domain for non-commercial purposes, and revoke the privacy feature with evidence of commercial use such as a commercial Web site or email. We encourage ICANN to use this proven common sense approach. While we doubt that any legitimate applicant would ever use the "maximum privacy feature," so long as it's treated as a rare exception, we wouldn't find it to be objectionable per se.

Our main concern is about Gated Access, which appears to proceed on the assumptions that most Internet users have no security concerns that merit access to detailed WHOIS data, and that it is possible to identify and certify the users that do. Both assumptions are wrong. The vast majority of Internet users have never registered a domain and never will, while (as noted above) of the minority that do register, most of those are commercial without a reasonable expectation of privacy. Nobody can predict all of the legitimate reasons that someone might research WHOIS information, and it is an insult to the non-registrant majority to demand that they justify their interest in what is (and should remain) primarily public information about commercial entities. When a consumer wonders who is behind an email or Web site, or an email service provider wonders if a potential new customer is actually an undesirable former old customer under a new name, WHOIS searches are a routine and useful part of finding the answer. Does that make them security researchers? Should they have to justify their interest? Regardless of the answer to the first question, we believe the answer to the latter question is clearly no.

Furthermore, many of our members and our members' employees participate daily in a wide variety of security research activities, both within industry and jointly with governments and non-profits. We can report from our direct experience that it is impossible to define who is a "legitimate" security researcher. Indeed, in the government fora it's remarkably hard even for a group of government enforcement officers to tell who their peers are in governments in other countries. This is not an area in which ICANN has, or should need, expertise, and we strongly believe that ICANN should *not* attempt to distinguish WHOIS users by the perceived legitimacy of their interest. Rather, it should set limits on access based on the actual use of the data, e.g., no use for marketing or building dossiers of personal information.

Please address any questions or requests for additional information to Jerry Upton, M3AAWG Executive Director at jerry.upton@m3aawg.org

Yours truly,
s/s
Jerry Upton, Executive Director, M3AAWG