MAAWG

To: Internet Corporation for Assigned Names and Numbers (ICANN)
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: April 14, 2011
Subject: Comments on ICANN WHOIS Review Team

To whom it may concern:

Thank-you for the opportunity to comment on the ICANN WHOIS Review Team.

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight online abuse such as phishing, botnets, fraud, spam, viruses and denial-of-service attacks. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (http://www.MAAWG.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards and the facilitation of global collaboration.

Usability of WHOIS service

MAAWG members often use WHOIS as a critical component of their work in the security realm. Not only should it be possible to obtain registration information for any DNS domain or network assignment, but that information should be available in a standard form with a consistent set of parameters reported on each entity, as "thick" WHOIS service does. At present, the content of a WHOIS reply from a "thin" WHOIS does not report a consistent set of fields using a consistent format, making use of the data by automated entities difficult. Moreover, queries from a single customer are often rate-limited, preventing any automated use of the system for registrant assessment.

MAAWG recommends that ICANN require all registries transition to a "thick" WHOIS service. This will provide reliable service and standardized report formats.

Access to WHOIS

We firmly oppose any proposal allowing only law enforcement agencies access to WHOIS or a subset thereof. The vast majority of the abuses on the Internet – be it spam, phishing, malware hosting, copyright violations, denial-of-service attacks and so on – are not dealt with by law enforcement who, when they are engaged, must allocate their precious resources to only the most egregious of cases. In some jurisdictions, many of these issues remain entirely outside the scope of law enforcement. For example, Spain only recently passed a law dealing with botnets. Prior to the law, bots were entirely legal.

The fact of the matter is that these issues are dealt with by security and systems administration professionals, in cooperation with, but often independently of, law enforcement. WHOIS is a critical component in the ability of security professionals to make the Internet a safer place for end users.

Ensuring accuracy and reliability of WHOIS service

We believe un-obfuscated WHOIS must be as robust and highly available as the DNS, and certain data-points must be openly available to security-related assessment systems. This should be considered a mandatory minimum for implementations, registrars and registrants, and ICANN must enforce compliance with the rules for them to be meaningful. We understand the need for privacy of some individual (non-commercial) registrants, but the casual overuse of privacy proxies by commercial and criminal actors impairs the ability of security systems to make accurate assessments of incoming data to protect end users. We work, on a daily basis, to protect the privacy rights on tens of millions of end users, and we fail to see how the (often falsely) asserted privacy rights of a commercial enterprise can trump them.

Improvement of WDPRS

When missing or inaccurate WHOIS information is detected, users have the option of reporting that inaccuracy via the WHOIS Data Problem Reporting System (http://wdprs.internic.net/). Unfortunately that system is operationally cumbersome, requiring domain-by-domain reporting via a Web form, followed by email confirmations, even in cases where hundreds or thousands of domains share the same inaccuracies. We understand that an authenticated bulk interface is in use by a small number of reporters and recommend that it be made available to the public under reasonable and nondiscriminatory conditions.

In the spirit of operational transparency, ICANN should also provide quarterly reports summarizing the number of WDPRS reports received, the registrars those reports pertain to, the nature of the inaccuracies, and the disposition of those reports as reported in the solicited WDPRS follow-up surveys.

Abuse of WHOIS service

The WHOIS Policy Team is focused on the erosion of trust in the WHOIS service, as the publication of identifying data means that data can be abused. We agree but single-use email addresses or a similar technical scheme is an appropriate way to limit spam to WHOIS points of contact; obfuscating or making inaccessible the WHOIS database is throwing the baby out with the bathwater.

Lastly, there has been little emphasis placed on technological improvements to the WHOIS service, something that is sorely needed. We hope that the WHOIS Review Team will take improvements, such as those made by ARIN, into consideration in their final report.

Sincerely,
Jerry Upton, Executive Director
Messaging Anti-Abuse Working Group