Request for Proposals for
WHOIS Privacy and Proxy Abuse Studies

* Deadline for applications 20 July, 2010*

1. Introduction

1.1. The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation responsible for coordinating critical Internet resources. These include Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain Name System (DNS) management, and root server system management. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

As part of its work, ICANN develops policy for WHOIS services that provide public access to data about registered domain names. The extent of data collected at the time of domain name registration, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in gTLDs.

For example, ICANN requires accredited registrars to collect and provide free public access to the name of the registered domain name and its name servers and registrar, the date the domain was created and when its expires, and the contact information for the domain name's Registered Name Holder, technical contact, and administrative contact. Anyone can obtain this data by using a WHOIS client to send an RFC 3912-formatted query to TCP port 43, or by submitting a web form query to a WHOIS server. Data is returned in an unspecified human-readable form, predominately but not exclusively represented in US-ASCII.

The Generic Names Supporting Organization (GNSO) is responsible for developing and recommending to the ICANN Board substantive policies relating to gTLDs. The GNSO Council is now exploring several extensive studies of WHOIS and has asked ICANN to estimate the cost of conducting several studies proposed by members of the ICANN community and Government Advisory Committee.

1.2. Pursuant to the above request, ICANN seeks to engage independent research organizations to undertake one or more proposed WHOIS Privacy and Proxy Abuse studies. The information outlined below illustrates the scope of work and the criteria for selection.

1.3. This document should be read in conjunction with the Terms of Reference for WHOIS Privacy and Proxy Abuse Studies document (also found at http://gnso.icann.org/issues/whois/index.html). Read together, these two documents provide the materials necessary to respond to this Request for Proposals ("RFP") for WHOIS Privacy and Proxy Abuse Studies.

2. Objectives

2.1. WHOIS Privacy and Proxy Abuse studies are designed to methodically analyze a representative sample of gTLD domains associated with a variety of illegal/harmful Internet activities. By measuring how often these alleged and confirmed "bad actors" use Privacy/Proxy registrations, compared to the overall frequency of Privacy/Proxy registrations, this study will attempt to prove or disprove the following hypothesis: *A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.*

Here, "illegal or harmful communication" refers to online activities (e.g., email messages, web transactions, file downloads) that violate criminal or civil law or which harm their targets (e.g., email/file recipients, website visitors). Allegations of actionable harm may require victims, law enforcement officials, and others to contact domain owners or licensees. Some have suggested that Privacy/Proxy services are being abused to obscure the identity of perpetrators that instigate illegal/harmful communications, thereby impeding investigation. To provide the ICANN community with empirical data to evaluate such concerns, these studies will examine a representative sample of illegal/harmful incidents to measure how often Privacy/Proxy services are in fact abused by perpetrators (both alleged and confirmed).

2.2. ICANN will provide the successful candidate with background documentation and reports pertaining to these and other WHOIS studies. Applicants are encouraged to explicitly identify any assumptions or dependencies they may have with respect to support required from ICANN and other organizations. In particular, these studies will use a representative sample of "bad actor" domain names to be supplied by organizations that routinely track, investigate, and/or remediate various kinds of illegal/harmful activities.

- Domain names associated with short-lived illegal/harmful Internet activities should ideally be collected from reputable live-feed sources. Possible sources are listed in the Terms of Reference; researchers are expected to refine and finalize this source list during the first phase of the study.

- Domain names associated with less time-critical illegal/harmful activities can be gathered from third-parties that routinely respond to or track such incidents in large volume and might be willing to assist by recording WHOIS data early in their investigation. Possible participants are listed in the Terms of Reference; researchers are expected to refine and finalize this list during the first phase of the study.

Applicants are invited to elaborate upon possible sources/participants, viable methods for interacting with these organizations, and any dependencies on ICANN to facilitate this interaction.

2.3. If ICANN elects to conduct WHOIS Privacy and Proxy Abuse studies, they are not likely to begin until 2011. Applicants are requested to propose timelines that reflect tasks and durations without requiring a specific start date. A full project timeline will be developed before the study is launched. It is anticipated that a key milestone will include presentation of preliminary study findings at an upcoming ICANN public meeting. Final study findings will also be posted for public review and comment.

2.4. Research organization(s) that conduct these studies are expected to have detailed knowledge of and experience with conducting global Internet threat research studies. Some familiarity with DNS, WHOIS, and Privacy/Proxy registration services is also required, including policies regarding access to and permissible use of domain name registration data.

3. Tender Scope and Conditions

3.1. Taking note of the Terms of Reference, applicants should provide the following:

3.1.1. Statement of Suitability. The Statement of Suitability must include a detailed outline of the applicant's ability to perform this work, including references and examples of past research projects, publications, and other relevant information. Preference will be given applicants who can demonstrate experience conducting Internet threat research in general and DNS, WHOIS, and Privacy/Proxy services in particular.

3.1.2. Work Approach. The Work Approach needs to detail the way in which the applicant would respond to the Terms of Reference, providing details about how the specified study would be conducted. Applicants are encouraged to elaborate upon the study definitions summarized in the Terms of Reference as needed to quantify effort, enumerate assumptions, and identify dependencies.

The successful candidate will be expected to interact with ICANN via email, conference calls, and video conference to refine proposed study methodologies, finalize input sources/participants, and review study progress. The successful candidate will be expected to present draft study findings in person at one of ICANN's public meetings.

3.1.3. Team Curriculum Vitae. The response must include Curriculum Vitae for key personnel who will lead and conduct each study, showing each individual's suitability for the proposed work. Given the nature of these studies, the successful candidate will need to apply staff with specific skills to certain tasks (e.g., a team familiar with live-feeds, ability to communicate with non-English speaking participants).

3.1.4. ICANN Contract Compliance. Applicants should warrant that they are willing to operate under a non-disclosure agreement.

3.1.5. Schedule and Fees. The proposal should include a work schedule, including key milestone dates and a statement of proposed fees. Fees should be inclusive of related project expenses, including (but not limited to) electronic, postal, and telephone communication; computer hardware, software, and services; and travel costs.

3.2. **Deadline / Requirements:** By July 20, 2010, interested applicants should submit proposals by email to rfpwhois@icann.org to the attention of Liz Gasster, Senior Policy Counselor, ICANN Policy Department. A confirmation email will be sent for each proposal received.