ICANN

Request for Proposal
For
Study on Rates of DNS Abuse in New and Legacy Top-Level Domains

Date of issue 2 August 2016

1.0 Introduction

1.1 About this Document

The Internet Corporation for Assigned Names and Numbers' ("ICANN") New Generic Top-Level Domain (gTLD) Program has enabled hundreds of new generic top-level domains to enter into the domain name system (DNS) since the first delegations occurred in October 2013. gTLDs are the domain name extensions like the familiar .COM, .NET or .ORG. The New gTLD Program ("Program") was developed via ICANN's multi-stakeholder process to increase competition and choice in the domain name space. More than 1,900 applications for new gTLDs were filed after the process opened in 2012. To date, more than 1,000 new gTLDs have been delegated into to the DNS' root zone.

A number of safeguards were built into the Program that were intended to mitigate rates of abusive, malicious, and criminal activity in these new gTLDs, such as **phishing, spam, malware distribution, and botnet command-and-control**. ICANN is currently engaged in a review of these safeguards and their effects on rates of DNS abuse, and is **seeking a provider to conduct a study examining rates of malicious and abusive behavior in the global DNS**.

A multi-stakeholder community review team will make use of the findings as one input into its review of ICANN's New gTLD Program and its impact on competition, consumer trust, and consumer choice. The review may also inform recommendations to ICANN on additional initiatives that should be undertaken. In particular, this DNS Abuse study will serve as a gauge for the extent of DNS abuse occurring in new gTLDs, which in turn will help inform the review team's mission to assess the New gTLD Program's impact on consumer trust.

As the DNS represents a large ecosystem of registries, registrars, domain name resellers, privacy/proxy service providers, the study must be able to capture inputs in a representative manner from across the multitude of players relevant to abusive practices.

1.2 Overview of the Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers' (ICANN) mission is to help ensure a stable, secure and unified global Internet. To reach another person on the Internet, you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world.

See www.icann.org for more information.

2.0 DNS Abuse Study Overview

2.1 Project Objective

The objective of this RFP is to identify a qualified supplier to conduct a study of DNS abuse in new and legacy gTLDs. A complete project timeline is available in the Project Timeline section below.

2.2 Background of the RFP

As part of its Affirmation of Commitments ("Affirmation"), ICANN has pledged to promote competition, consumer trust, and consumer choice in the domain name marketplace. The Affirmation outlines ICANN's responsibilities to the global community of Internet users, who are all served by the DNS. The Affirmation focuses on three primary areas: (a) ensuring accountability, transparency and the interests of global Internet users; (b) preserving security, stability and resiliency of the DNS; and (c) promoting competition, consumer trust and consumer choice.

The Affirmation commits ICANN to undertake a comprehensive review of the New gTLD Program in each of these areas. The mandate for the DNS Abuse study stems from section 9.3 of the Affirmation, which states: "ICANN will organize a review that will examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of (a) the application and evaluation process, and (b) safeguards put in place to mitigate issues involved in the introduction or expansion" [emphasis added]. The DNS Abuse study will serve as a foundational input on this final provision to help the review team evaluate the effectiveness of those safeguards in mitigating DNS abuse.

2.3 Scope of Work

The work is expected to entail two components: 1) a comprehensive descriptive statistical comparison of rates of DNS Abuse in new and legacy gTLDs as they pertain to spam, phishing, malware distribution, and botnet command-and-control, and 2) two inferential statistical analyses testing 1) the correlation between domain name retail pricing as a predictor of rates of abuse [1] and 2) the correlation between the deployment of Domain Name Security Extension protocols (DNSSEC) in top- and second-level domains as a predictor of rates of abuse.

In sum, the work can be divided into two primary components:

[1] Domain name retail pricing is widely hypothesized to be a predictor of DNS abuse rates in the literature on the subject and among subject matter experts in the ICANN community.

1. A *descriptive* statistical analysis of abuse rates that makes use of data sources such as, but not limited to, historical zone files, WHOIS data, and domain blocklist data
2. Two *inferential* statistical analyses examining:
    a. The correlation between domain name retail pricing and abuse rates
    b. The correlation between the deployment of DNSSEC and abuse rates

Potential suppliers are encouraged to submit proposals to address both components. However, given the timeframe of the proposed study, potential suppliers may submit proposals to address one of these components as described, with high priority assigned to the first component. Preference will be given to suppliers addressing both components; however, separate contracts may be awarded to separate suppliers for each component of the study depending on the focus of proposals.

<u>Component 1: Descriptive Statistical Analysis</u> (high priority)

1. Utilize zone file data for all new and legacy gTLDs from 1 January 2014 to present to assess:
    a. The overall number of domain names registered in each TLD zone
    b. Time to live for domain names (timeframe from when domain names are registered to when they are used for abuse and ultimately suspended, as applicable)
2. Utilize historical WHOIS data from 1 January 2014 to present to determine the main sources of abusive registrations, categorized by TLD, registrar, resellers, and privacy/proxy service provider.
3. Combine DNS abuse data obtained from reputable DNS abuse monitoring services (i.e. domain blocklists) from 1 January 2014 to present with zone file and historical WHOIS data to determine the distribution of abusive activities across the DNS industry and segmented by abusive activity, as described in Introduction.

<u>Component 2: Inferential Statistical Analysis</u>

1. Statistically test the hypothesized relationship between domain name retail pricing as a predictor of rates of DNS abuse in new and legacy gTLDs.
2. Statistically test the hypothesized relationship between the deployment of DNSSEC at the top- and second-levels of the DNS as a predictor of rates of DNS abuse in new and legacy gTLDs.

2.4 Work Deliverables

In general, the final report will:

- Provide a robust and comprehensive comparison of abuse rates in new and legacy gTLDs
- Provide thorough description of methodology and data sets that conforms to academic standards of such reporting
- Contain graphical representations of descriptive analyses as appropriate
- Provide thorough statistical significance testing in inferential statistical analyses that conform to academic standards of such reporting
- Ensure the analysis accounts for the size of the TLD and the proportion of specific TLDs that a registrar, reseller, or privacy/proxy service sells, and overall abusive registration frequency for the TLD itself and for registrars, resellers, and privacy/proxy services.

Specifically, the final report will provide:

Component 1: Descriptive Analysis

1. Overall numbers of abusive domains per TLD, registrar, reseller, privacy/proxy service, and geographic region from 1 January 2014 to present, segmented according to the abuse activities described in the Introduction.
2. Proportion of abusive domains per TLD, registrar, reseller, privacy/proxy service, and geographic region from 1 January 2014 to present, segmented according to the abuse activities described in the Introduction.
3. An analysis whose timeframe incorporates the actual dates at which domain names for each new gTLD could resolve, distinguishing the sunrise period from general availability to capture the time frames in which abusive activity is most likely to occur (i.e. following the release of a domain name for general availability)
4. A determination of the average time to live for abusive registrations, broken down by TLD, registrar, reseller, privacy/proxy service, and geographic region in order to demonstrate whether some abusive second-level domains under each TLD remain registered longer than others before being taken down.

Component 2: Inferential Analysis

1. Robust and thorough statistical significance testing of the relationship between domain name retail pricing data over time and DNS abuse rates of over time, segmented—as feasible—according to the categories described in Introduction section.
2. Robust and thorough statistical significance testing of the relationship between the deployment of DNSSEC over time and the top- and second-level of the DNS

and DNS abuse rates of over time, segmented—as feasible—according to the abuse categories described in Introduction section.

Note that ICANN may be able to provide a number of data resources to the selected supplier, subject to all applicable terms of use. These may include:

1. Historical zone file and WHOIS data
2. Pricing data (as publicly available and/or as has been used in previous ICANN studies, as appropriate to terms of use)
3. Support for access to domain blocklist data feeds

Given their historical nature, some of these resources may have limited data and would thus require a targeted analysis of the information available. The specifics of this data provision and access will be discussed with the selected supplier during initial planning sessions.

3.0 High Level Selection Criteria

The decision to select a provider as an outcome of this RFP will be based on, but not limited to, the following selection criteria:

1. Demonstrated understanding of the assignment
2. Knowledge and expertise
    a. Demonstrated experience in conducting broadly similar studies
    b. Basic knowledge of ICANN functions, DNS, and the domain name registration process
    c. Suitability of proposed CVs
    d. Demonstrated expertise in conduct of descriptive and inferential statistical analysis
3. Proposed methodology
    a. Work organization, project management approach, timelines
    b. Suitability of tools and methods or work
    c. Clarity of deliverables
    d. If applicable, methodology and project management approach of any partner firms.
4. Flexible approach, including but not limited to meeting the timeline by launching work **17 October 2016** and finishing by **17 March 2017**, allowing for shifting definitions and incorporating community input.
5. Commitment to working with ICANN's multi-stakeholder model, including a demonstrated understanding of and commitment to ICANN's requirements for transparency and accountability.
6. Reference checks (see template), both for applicant and any partner firms

7. Conflict of interest (see template)

4.0 High Level Organizational Requirements

In order to be considered, the providers must be able to demonstrate ability to meet the following organizational requirements:

1. Ability to provide a complete response based on ICANN specifications by the designated due date (see timeline below).
2. Availability to participate in finalist presentations via conference call/remote participation (see timeline below).
3. Ability to negotiate a professional services agreement using ICANN Contractor Consulting Agreement (see attached).
4. Ability to begin work on **17 October 2016** and complete it by **17 March 2017**.
5. Conduct periodic update calls, frequency to be determined.
6. Demonstrated ability to develop work methods, data gathering mechanisms and evaluation/assessment approaches as appropriate to the study.
7. Able to produce work plan and timeline.
8. Working session(s), as necessary, with the ICANN representatives and/or community Review Team members to discuss preliminary findings (via remote participation).
9. Ability to travel to attend 1 face-to-face meeting with Review Team to present results.
10. Able to produce draft report with preliminary findings by **2 January 2017** (draft report to include methodology and approach, preliminary assessment of available objective and quantifiable findings, and preview of expected findings).
11. Able to produce a final report by **17 March 2017**, based on responses to clarifying questions and comments from ICANN. Organization's representatives may be asked to present findings to ICANN's multi-stakeholder community.

5.0 Project Timeline

The following dates have been established as milestones for this RFP. ICANN reserves the right to modify or change this timeline at any time as necessary. All responses (including proposals, supporting documentation, questions, etc.) must be submitted via the ICANN Sourcing Tool. Access to the ICANN Sourcing Tool may be obtained by sending a request to dnsabuse-study-rfp@icann.org .

Activity	Dates
RFP published	2 August 2016
Participants to indicate interest and submit any questions to ICANN via the ICANN Sourcing	12 August 2016 by 23:59 UTC

tool	
ICANN responds to participant questions	19 August 2016
Participant RFP proposals due by	**25 August 2016 by 23:59 UTC**
Initial evaluation of responses	26 August thru 10 September 2016
Supplier presentations including Q&A via conference call/remote participation with shortlisted candidates	13 thru 16 September 2016
Final evaluations and selection of supplier (includes negotiations, contracting and award)	19 September thru 14 October 2016
Estimated start of study	**17 October 2016**
Draft report with preliminary findings due	2 January 2017
Final report due (incorporating revisions and updated research findings)	17 March 2017

6.0 Terms and Conditions

General Terms and Conditions

1. Submission of a proposal shall constitute Respondent's acknowledgment and acceptance of all the specifications, requirements and terms and conditions in this RFP.

2. All costs of preparing and submitting its proposal, responding to or providing any other assistance to ICANN in connection with this RFP will be borne by the Respondent.

3. All submitted proposals including any supporting materials or documentation will become the property of ICANN. If Respondent's proposal contains any proprietary information that should not be disclosed or used by ICANN other than for the purposes of evaluating the proposal, that information should be marked with appropriate confidentiality markings.

Discrepancies, Omissions and Additional Information

1. Respondent is responsible for examining this RFP and all addenda. Failure to do so will be at the sole risk of Respondent. Should Respondent find discrepancies, omissions, unclear or ambiguous intent or meaning, or should any question arise concerning this RFP, Respondent must notify ICANN of such findings immediately in writing via e-mail no later than three (3) days prior to the deadline for bid submissions. Should such matters remain unresolved by ICANN, in writing, prior to

Respondent's preparation of its proposal, such matters must be addressed in Respondent's proposal.

2. ICANN is not responsible for oral statements made by its employees, agents, or representatives concerning this RFP. If Respondent requires additional information, Respondent must request that the issuer of this RFP furnish such information in writing.

3. A Respondent's proposal is presumed to represent its best efforts to respond to the RFP. Any significant inconsistency, if unexplained, raises a fundamental issue of the Respondent's understanding of the nature and scope of the work required and of its ability to perform the contract as proposed and may be cause for rejection of the proposal. The burden of proof as to cost credibility rests with the Respondent.

4. If necessary, supplemental information to this RFP will be provided to all prospective Respondents receiving this RFP. All supplemental information issued by ICANN will form part of this RFP. ICANN is not responsible for any failure by prospective Respondents to receive supplemental information.

Assessment and Award

1. ICANN reserves the right, without penalty and at its discretion, to accept or reject any proposal, withdraw this RFP, make no award, to waive or permit the correction of any informality or irregularity and to disregard any non-conforming or conditional proposal.

2. ICANN may request a Respondent to provide further information or documentation to support Respondent's proposal and its ability to provide the products and/or services contemplated by this RFP.

3. ICANN is not obliged to accept the lowest priced proposal. Price is only one of the determining factors for the successful award.

4. ICANN will assess proposals based on compliant responses to the requirements set out in this RFP, any further issued clarifications (if any) and consideration of any other issues or evidence relevant to the Respondent's ability to successfully provide and implement the products and/or services contemplated by this RFP and in the best interests of ICANN.

5. ICANN reserves the right to enter into contractual negotiations and if necessary, modify any terms and conditions of a final contract with the Respondent whose proposal offers the best value to ICANN.