Internet Corporation for Assigned Names and Numbers (ICANN)

Request for Proposal - Global Background Screening Services

2011 August 30

1.0 Introduction

1.1 About this Document

By issuing this Request for Proposal ("RFP"), the Internet Corporation for Assigned Names and Numbers ("ICANN") is requesting your best offer to provide a response to the requirements of a global background screening process for new generic top level domain (gTLD) applicants. In seeking a comprehensive agreement for these services, ICANN is placing maximum emphasis on several key components of value, including expertise with global and local screening processes, demonstrated practices, value-added services, and the ability to work within the guidelines established in this RFP.

1.2 Overview of ICANN

The mission of ICANN, pursuant to its bylaws, is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
    a. Domain names (forming a system referred to as "DNS");
    b. Internet Protocol ("IP") addresses;
    c. Autonomous System ("AS") numbers; and
    d. Protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately related to these technical functions.

ICANN is dedicated to preserving the operational security and 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.

See www.icann.org for more information.

1.3 Overview of the Initiative

New gTLDs have been in the forefront of ICANN's agenda since its creation. The new gTLD program will open up the top level of the Internet's namespace to foster diversity, encourage competition, and enhance the utility of the DNS.

Currently the namespace consists of over 20 gTLDs and over 200 ccTLDs operating on various models. Generally, each of the gTLDs has a designated "registry operator" according to a Registry Agreement between the operator (or sponsor) and ICANN. The registry operator is responsible for the technical operation of the TLD, including all of the names registered in that TLD. gTLDs are served by over 900 registrars, who interact with registrants to perform domain name registration and other related services.

The new gTLD program will create a means for prospective registry operators to apply for new gTLDs, and create new options for consumers in the market. When the program launches its first application round, ICANN expects a diverse set of applications for new gTLDs, including Internationalized Domain Names (IDNs), creating significant potential for new uses and benefit to Internet users across the globe.

The program has its origins in carefully deliberated policy development work by the ICANN community. In October 2007, the Generic Names Supporting Organization (GNSO)—one of the groups that coordinate global Internet policy at ICANN—formally completed its policy development work on new gTLDs and approved a set of 19 policy recommendations. Representatives from a wide variety of stakeholder groups—governments, individuals, civil society, business and intellectual property constituencies, and the technology community—were engaged in discussions for more than 18 months on such questions as the demand, benefits and risks of new gTLDs, the selection criteria that should be applied, how gTLDs should be allocated, and the contractual conditions that should be required for new gTLD registries going forward. The culmination of this policy development process was a decision by the ICANN Board of Directors to adopt the community-developed policy in June 2008. A thorough brief to the policy process and outcomes can be found at http://gnso.icann.org/issues/new-gtlds.

ICANN's work is now focused on implementation: creating an application and evaluation process for new gTLDs that is aligned with the policy recommendations and provides a clear roadmap for applicants to reach delegation, including Board approval. This implementation work is reflected in the drafts of the applicant guidebook (see http://www.icann.org/en/topics/new-gtlds/comments-7-en.htm) that have been released for public comment, and in the explanatory papers giving insight into rationale behind some of the conclusions reached on specific topics. Meaningful community input has led to revisions of the draft applicant guidebook. In parallel, ICANN is establishing the resources needed to successfully launch and operate the program.

Mitigating the risk of "bad actors" entering the space by securing a gTLD is of considerable importance. ICANN has designed the new gTLD program with multiple stakeholder protection mechanisms. Background screening, features of the gTLD Registry Agreement, data and financial escrow mechanisms are all intended to provide registrant and user protections.

The purpose of this Request for Proposal (RFP) is to secure global background screening services. The background screening will focus on general business diligence, criminal history, and history of cybersquatting behavior. The scope of the background screening is expected to

cover, at a minimum, the entity applying as well as key directors, officers, partners, and major shareholders of that entity. Applicants are required to identify these individuals as part of completing the application.

Section 2.0 Objectives, Scope, and Requirements

2.1 Objectives

ICANN desires to engage a single provider of background screening services to provide a cost-effective and timely mechanism for ICANN to conduct background checks on applicants applying for critical Internet resources. The background screening will focus on general business diligence, criminal history, and cybersquatting behavior. The criteria used for criminal history are generally aligned with the "crimes of trust" standard sometimes used in the banking and financing industry.

2.2 Background Screening Scope

The gTLD application program is expected to receive approximately 300 to 500 applications in the first round with applications coming from varying organizational types (e.g., corporate, not-for-profit, government agencies, etc.) and various regions/countries. The selected vendor will be expected to deliver a background screening report that provides substantial guidance to ICANN as it considers each gTLD application. The scope of the background screening check is limited to convictions or decisions of the following crimes/offenses:

a. Within the past ten years, has been convicted of any crime related to financial or corporate governance activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that is substantially equivalent to these;
b. Within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of the funds of others;
c. Within the past ten years has been convicted of any willful tax-related fraud or willful evasion of tax liabilities;
d. Within the past ten years has been convicted of perjury, forswearing, failing to cooperate with a law enforcement investigation, or making false statements to a law enforcement agency or representative;
e. Has ever been convicted of any crime involving the use of computers, telephony systems, telecommunications or the Internet to facilitate the commission of crimes;
f. Has ever been convicted of any crime involving the use of a weapon, force, or threat of force;
g. Has ever been convicted of willful neglect or any violent or sexual offense victimizing children, the elderly, or individuals with disabilities;

h. Has ever been convicted of the illegal sale, manufacture, or distribution of pharmaceutical drugs, or been convicted of successfully extradited for any offense described in Article 3 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988*;
i. Has ever been convicted or successfully extradited for any offense described in the United Nations Convention against Transnational Organized Crime (all protocols)*
j. Has been convicted, within the respective timeframes, of aiding, abetting, facilitating, enabling, conspiring to commit, or failing to report any of the crimes listed above (i.e., within the past 10 years for crimes listed in a. through d. or ever for the crimes listed in e. through i.);
k. Is the subject of a disqualification imposed by ICANN and in effect at the time the application is considered;
l. Fails to provide ICANN with the complete and accurate identifying information necessary to confirm identity at the time of application or to resolve questions of identity during the background screening process;
m. Has been involved in a pattern of adverse, final decisions indicating that the applicant or individual named in the application was engaged in cybersquatting as defined in the Uniform Dispute Resolution Process (UDRP), the Anti-Cybersquatting Consumer Protection Act (ACPA), or other equivalent legislation or was engaged in reverse domain name hijacking under the UDRP or bad faith or reckless disregard under the ACPA or equivalent legislation. Three or more such decisions with one occurring in the last four years will generally be considered to constitute a pattern.
n. Has had a final and legally binding decision obtained by national law enforcement or consumer protection authority finding that the applicant was engaged in fraudulent and deceptive commercial practices as defined in the Organization for Economic Co-operation and Development (OECD) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders.

* It is recognized that not all countries have signed on to the UN conventions referenced above. These conventions are being used solely for identification of a list of crimes for which background screening should be performed. It is not necessarily required that the entity or individual would have been convicted pursuant to the UN convention but merely convicted of a crime listed under these conventions.

2.3 Required Capabilities & Experience

ICANN expects that respondents will, at a minimum, satisfy the following experience requirements:

1. Demonstrated ability to conduct international, regional, national, domestic, and local records checks including, but not limited to, criminal and civil courts, law enforcement agencies and regulatory authorities and any and all entities that are capable of providing such data in all countries where such records are available.
2. Possess a thorough knowledge of global, regional, and country specific screening processes
3. Have a demonstrated ability to provide background screening services in an expedited, orderly, and consistent manner
4. Have an excellent track record of performing background screening activities with competence at global, regional and country specific levels
5. Have the ability to scale quickly to meet the demands of an unknown number of applications (i.e., entities applying and key individuals listed) while meeting the time requirements to provide complete reports
    - The total number of applications in the first round is expected to range from 300 to 500. Note, anything above 500 will result in the processing of batches no greater than 500 at a time.
    - Background screening will be required for greater than 15% shareholders and key directors, officers and partners – each application is expected to have approximately 8 to 12 key individuals that will require background screening.
    - Background screening reports for all applications must be completed and sent to ICANN within 4 to 8 weeks of being submitted for background screening. Note, there is a possibility that all applications may be submitted for background screening at the same time.
6. Utilize processes that are compliant with all legal, privacy and data retention requirements in the various jurisdictions involved.
7. Familiarity with international criminal laws and treaties regarding fraud, corrupt practices (FCPA), computer abuse (such as spam and copyright violations), telecommunications, and Internet and experience performing background checks where knowledge of such laws is required
8. Provide a report that integrates with other sources of information as needed. For example, Uniform Dispute Resolution Providers (UDRP), the primary sources of data on cybersquatting complaints, may maintain data separately from general background screening sources. Accordingly the provider must be able to integrate with such sources of information to provide a single background screening report
9. Established resources to conduct more in-depth investigations on an international basis as needed.

Section 3.0 Required Response Items

3.1 Executive Summary

1. What characteristics most distinguish your organization from your competitors?
2. Summarize the key points of the proposal including the benefits to the Internet community of engaging your organization

3.2 Company Information and Background

1. Respondents must provide the following information regarding the organization:
    a. Name
    b. Street Address
    c. City
    d. State, Province or Region
    e. Country of Corporate headquarters
    f. Postal code(s)
    g. Country of Incorporation, if different
    h. Phone
    i. Fax
    j. Website
2. Please indicate if the organization is a subsidiary of any other company?
    a. If so, please indicate the parent company and how you are managed by the parent (actively or autonomously)
3. Please indicate if you are an affiliate of (or have as a client) any ICANN accredited registrar, registry or other contracted party or have any ownership interest in any ICANN accredited registrar, registry or other contracted party with ICANN
4. Please indicate if you provide any advisory or consulting services to potential Applicants or service providers expecting to participate in the New gTLD Program.

3.3 Qualifications, Approach, Timing and Estimated Costs

1. Provide an overview of the global resources of your organization including an overview of where you have offices
2. Provide examples of any relevant thought leadership, background screening industry participation, and publications that highlight your experience
3. Identify the internal processes which keep your organization abreast of relevant background screening industry issues/trends, including any thoughts on keeping ICANN informed of such trends
4. Describe the communication processes that will keep ICANN timely informed of background screening reports
5. Describe your organization's qualifications to deliver the required background screening services including addressing the scoping and experience requirements summarized in Sections 2.2 and 2.3
6. Background screening will begin soon after the posting of applications by ICANN. Background screening is key step in the overall evaluation of each application and must be completed timely to ensure ICANN is able to meet all defined timelines. In no case can initial background check take longer than 10 weeks to complete. Describe how your organization will be able to meet this time requirement. Include a description of the background screening lifecycle - from start to finish
7. Describe the proposed processes to be followed, including guiding principles, critical events, and quality control mechanisms. Also include your plan for integrating with ICANN's gTLD application process including what data is required and how data and reports will be shared between ICANN and your organization
8. Describe how the organization will conduct its research on the items listed in section 2.2 of this RFP including its ability to globally scale. Please list:
    a. The name and description of any organizations that will participate in the delivery of the services
    b. The sources of data that will be used
    c. How regional and local screening services are integrated
    d. How courts, government bodies, and regulatory agencies are integrated
    e. How other sources of information (e.g., UDRP providers) are integrated
9. Describe your organization's process for ensuring background check practices and results are current
10. Describe the process for determining and reporting any potential conflicts of interest between your organization and any entity or individual upon which a background screening check will be conducted. Note, a conflict with an entity or individual will cause the background screening to be conducted by another provider

11. Describe the team that will manage and execute the background screening process. Please include
    a. The organizational structure of the team
    b. Roles and responsibilities for each key team member
12. Describe any limitations or caveats for additional use of background screening reports once delivered, e.g., posting for public view or providing to the applicant directly
13. Please describe any process that would enable a risk ranking to be assigned to the application based on the background screening results
14. Describe the various reporting options available, including what distinguishes each type (i.e., depth of analysis, sources used, etc.), which can be used or tailored to meet ICANN's needs. Also identify the recommended report option based on the parameters described in this RFP
15. Provide a sample background check report(s) for a fictitious entity, that would meet the above criteria for varying report types
16. Provide estimated costs per report for the various reporting options assuming 100, 500, and 1,000 applications. Any start up costs should be separately stated and a description of such costs, including the expected time required to ramp up, should also be listed. Note, the start up costs and cost per report will be a major factor in selecting the appropriate vendor
17. Some organizations or individuals named in one application may be included in other applications or an organization may submit several applications. Please describe a process for minimizing or eliminating duplicative background screening costs.
18. Provide the approach and incremental cost to conduct additional research (i.e., from one reporting type to the next higher level and beyond the highest reporting level listed) for an Application on an as-needed basis
19. Describe the quality control process that would prevent your company from breaking any international, regional, national, domestic, and/or local laws in conducting your research
20. Describe the quality control processes that would ensure your company validates and verifies any and all material obtained from the Internet - for example searches conducted via general Internet search engines, and closed databases to which only limited organizations, such as yours, may have access.

Section 4.0 Instructions to Respondents

4.1 Definition of Respondent

"Respondent" means any person or firm receiving this RFP or submitting a proposal in response to this RFP.

4.2 Timeline

The following dates have been established as milestones for this RFP. ICANN reserves the right to modify or change this timeline in its absolute discretion.

This is a general timetable for the written proposal process, and possible oral presentations.

Request for proposals issued	30 August 2011
Written proposals due	4 October 2011
Last day to submit questions regarding RFP (Send to BackgroundScreeningRFP@icann.org)	13 September 2011
Answers to questions	22 September 2011
Selection of short-list vendors	7 October 2011
Selection of vendor	21 October 2011
Public announcement of selection	31 October 2011

4.3 Submission of Proposals

Proposals shall be prepared and submitted in the number, form and format requested by this RFP. Your written proposal should include responses to each of the attached RFP questions. For ease of evaluation, please limit your response to no more than 35 pages, plus necessary appendices, including team resumes. Please arrange to have an electronic copy delivered to mailto:backgroundscreeningrfp@icann.org by 23.59 UTC on 4 October 2011.

4.4 Discrepancies, Omissions and Additional Information

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 email no later than three (3) days prior to the deadline for bid submissions to BackgroundScreeningRFP@icann.org.

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.

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.

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.

4.5 Proposal Evaluation

ICANN will evaluate Respondent's proposal and other pertinent information to arrive at an award decision. Respondent's entire proposal will be reviewed for responsiveness to the RFP and for clarity and conciseness of the information presented. ICANN will review the information presented to determine which proposal best meets the background screening criteria.

4.6 Selection of the Background Screening Provider

Respondent's proposal will be evaluated by a Selection Committee, using a comprehensive set of criteria. The proposal will be evaluated on the basis of its technical, management and cost merits after a review of all aspects of each category in relationship to the requirements of this RFP. The ultimate basis for the selection will be in the absolute discretion of ICANN.

A partial list of the evaluation criteria follows:

- Is the Respondent's proposed solution capable of meeting the objectives and requirements set forth in this RFP?
- Has the Respondent clearly demonstrated the fee structure to ensure a cost-efficient model?
- Are the Respondent's experience and capabilities clearly stated in the proposal?
- Does the Respondent have the experience to run such a program?
- Is approach clear and does it meet the background screening requirements?
- Has the Respondent demonstrated an ability to scale as necessary?
- Is the requested proposal complete and in the format requested?

Proposals are required to be valid for a minimum of one hundred twenty (120) days following the deadline for submission of the proposal. A proposal may not be modified, withdrawn or canceled by the Respondent for a 120-day period following the deadline for submission of the proposal. The Respondent so agrees to this condition by submission of the proposal.

4.7 Disclaimer

This RFP shall not be construed in any manner to create an obligation on the part of ICANN to enter into any contract, or to serve as a basis for any claim whatsoever for reimbursement of costs for efforts expended. The scope of this RFP may be revised at the sole option of ICANN at any time. ICANN shall not be obligated by any proposals or by any statements or representations, whether oral or written, that may be made by ICANN, except as provided for in a final approved signed agreement. ICANN shall be held free from any liability resulting from the use or implied use of the information submitted in any proposal. Submission of a proposal shall constitute Respondent's acknowledgment and acceptance of all the specifications and requirements in this RFP.