# Project Overview for the Grant Program RFP

Request for Proposal

5 June 2023

ICANN

# 1 Introduction

## 1.1 About this Document

This document provides an overview of the Request for Proposal (RFP) for the ICANN Grant Program. It includes background and pertinent information regarding the requirements for the respondents. The RFP itself is comprised of this as well as other documents that are hosted in the ICANN sourcing tool (SciQuest/Jaggaer). Indications of interest are to be received by emailing The-Grant-Program-RFP@icann.org. Responses should be electronically submitted by 7 July 2023 at 23:59 UTC using ICANN's sourcing tool, access to which may be requested via the same email address as above.

## 1.2 About 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 need to type an address – a name or a number – into your computer or other device. That address must be unique so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world. ICANN was formed in 1998 as a nonprofit public benefit corporation with a community of participants from all over the world.

See www.icann.org for more information.

# 2 Scope

## 2.1 Project Objective

The Internet Corporation for Assigned Names and Numbers ("ICANN") will evaluate vendor(s) for the provision of the services specified in this Request for Proposal (RFP) in support of the ICANN Grant Program.

This Program is being designed on the basis of best practices at the forefront. ICANN is looking for external vendors with a proven track record of expertise in the grant program environment to support its work and achieve the objective to deliver a top-standards program.

ICANN is recognized by the U.S. Internal Revenue Service as a tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code. ICANN is further recognized by the IRS as a public charity pursuant to Section 509(2)(a) of the Internal Revenue Code. Throughout the Program and in the context of the rendered services, vendors should show ability in monitoring for and assisting ICANN with compliance with the relevant regulations governing ICANN's tax-exempt status.

This RFP will be conducted with the objective of maximizing the benefit for the Program, while offering vendors a fair and equitable opportunity to participate. Elements such as cost of services and experience will be considered in the selection of vendor(s).

The Program will operate in a series of grant cycles until the funds are depleted. Each cycle includes, at minimum: development (or confirmation) of application materials; receipt of applications; validation of applications/applicants meeting admissibility and eligibility criteria; evaluation of applications by an Independent Application Assessment Panel; recommendation of a slate of applications to the ICANN Board of Directors; Board consideration of slate; contracting and disbursement of grants; auditing, reporting and monitoring on grants as appropriate; and evaluation of cycle to determine if future modifications are needed.

ICANN org is looking for vendor(s) that may be able to offer services in some or all of the following areas: assembling and managing the Independent Application Assessment Panel; conducting eligibility checks of applications received; offering and managing grant management software throughout the lifecycle of a grant, from the application phase through the end of the grant, as well as applicant and grantee support; and/or to conduct process/cycle evaluations for future improvements, as needed.

This Request for Proposal (RFP) is open/public (i.e. anyone may provide a response). The goal of the RFP is to identify competent vendors that can provide services for some, or all areas mentioned above. Evaluations from bids received during the RFP will ideally result in the selection of one or more vendors.

## 2.2 Background

The ICANN Grant Program is based on the recommendations contained in the Final Report of the Cross-Community Working Group on New gTLD Auction Proceeds (CCWG-AP), as adopted by the ICANN Board in its 12 June 2022 resolutions. These recommendations provided ICANN with guidance on the distribution of proceeds from the auctions of last resort in the 2012 New gTLD Program. This program is being designed with best practices at the forefront. Because this is a new program for ICANN, there is a need for external vendors with a proven track record of expertise in the grant-making field to support this work.

The CCWG-AP Final Report outlines the program objectives as:

- Benefit the development, distribution, evolution and structures/projects that support the Internet's unique identifier systems
- Benefit capacity building and underserved populations, or
- Benefit the open and interoperable Internet

New gTLD Auction Proceeds are expected to be allocated in a manner consistent with ICANN's mission.

ICANN is working to refine those objectives and translate them into work areas.

## 2.3 Scope of Work

We expect the vendor(s) to demonstrate the ability to deliver on one or more of the following services:

1. Grant management software to act as 1) the unique channel through which applications are uploaded/updated/submitted and the final report of a funded application is submitted 2) a repository for applications for the lifecycle of applications and beyond, 3) the primary channel for communication between ICANN org & applicants, 4) a conduit for assessing and reporting on granted application, 5) the tool to maintain records for the amount of the grants, selection criteria and eligibility determinations and other information required by US IRS Form 990, Schedule A, F and I. More details on this requirement can be found **under section 4 of this document**.
2. Performance of eligibility checks on the applicant. More in detail:
    a. Check that US-based applicants are United States organizations recognized by the Internal Revenue Service as described in section 501(c)(3) of the Internal Revenue Code. For non-US-based applicants, conduct expenditure responsibility and/or equivalency determination reviews.
    b. Applicant background check to ensure no previous financial mismanagement or other issues that could pose a reputational risk to ICANN or that suggest heightened risk of misuse of proceeds.
3. Management of the Independent Assessment Panel. More in detail:
    a. Assemble the Independent Application Assessment Panel based on the objectives of the ICANN Grant Program (**as highlighted in section 4 of this document**), and the criteria as defined by ICANN org.
    b. Manage/oversee the work of the Independent Application Assessment Panel and ensure compliance with Non-Disclosure Agreements (NDA) and Conflicts of Interest (CoI) practices, etc., as developed in cooperation with ICANN.
    c. Manage the assessment of the admissible and eligible applications by the Independent Panel according to the criteria as defined by ICANN org (**as highlighted in section 4 of this document**).

# 3 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. Capacity to and expertise in delivering/managing the grant management software.
2. Ability to monitor for and assist ICANN with compliance with its 501(c)(3) and 509(2)(a) status in the context of the rendered services.
3. Documented expertise in managing and/or supporting grant programs.
4. Technical environment & enterprise architecture standards.
5. Approach to infrastructure and security.
6. High levels of responsiveness to internal and external needs.
7. Pricing offered.
8. Mitigation of any conflicts of interest.
9. Value added services.

# 4 High Level Business Requirements

The provider must be able to adhere to the complete list of business requirements as listed in SciQuest/Jaggaer. A summary of the key business requirements is listed below:

1. Ability to communicate (verbally and in writing) in English.
2. Availability to participate in the meetings in person or via conference call/remote participation.
3. Ability to monitor for and assist ICANN with compliance to its 501(c)(3) status.

*Grant management software requirements.*

The vendor will have to offer and manage an English language-based grant management software solution that includes the following features:

1. A platform that handles all the components of the grant process, from the application phase to the evaluation stage, from the grant agreement phase to the funds disbursement, from the funded project monitoring and reporting to the project final report.
2. A ticketing system for communication between ICANN org & applicants within the grant management software.
3. A functionality to maintain records for the amount of the grants, selection criteria and eligibility determinations and other information required by US IRS Form 990, Schedule F.

4. A functionality that enables a user account to enter and submit more than one complete application.
5. A functionality to develop custom user interfaces for externally facing web properties (e.g., applicant portal).
6. A functionality for any applicant to save, make changes and return to the application form before its final submission.
7. A functionality for the applicant and ICANN to upload documents throughout the grant cycle.
8. The option to extend out of the box software with configurable off-the-shelf components for critical features (e.g., eligibility checks, General Data Protection Regulation (GDPR), etc).
9. A functionality to generate status reports, to get an overview of all the tasks being performed in multiple processes.
10. A cloud-based system that meets ICANN's Service Architecture and Infrastructure Requirements (see Appendix 1).

The vendor is expected to enter into a Service Level Agreement with ICANN.

ICANN utilizes the *OWASP Application Security Verification Standard (ASVS)* via the *InfoSec Guideline: Web App Security Verification Standards* as requirements and guidelines for web applications. During the RFP the vendor is not expected to reply to or complete this document, but instead, to provide what is expected for web application security practices for the final candidates. Please note, all web applications are expected to comply with Level 1 requirements, and web applications that handle sensitive data (ICANN propriety, PII, etc.) are expected to comply with Level 2.

*Independent Panel requirements*

The vendor will have to show:

1. Demonstrated ability to manage evaluation processes of international projects.
2. Demonstrated expertise in assembling and managing independent assessment panel(s) at international level. ICANN has the right to veto panelists.
3. Assessment of each application performed by a panel made of 3 to 5 panelists.
4. Assessment of each application against 3 to 6 evaluation criteria (as defined by ICANN) within the tentative time frame of three months.
5. Demonstrated robust Conflict of Interest policy for the panelists in place.
6. Demonstrated ability to develop work methods, evaluation/assessment approaches and reporting based on specific objectives and criteria.

*Applicant eligibility check requirements*

The vendor will have to:

1. Check that US-based applicants are United States organizations recognized by the Internal Revenue Service as described in section 501(c)(3) of the Internal Revenue

Code; for non-US-based applicants, conduct expenditure responsibility and/or equivalency determination reviews.

2. Run applicant background check to ensure no previous financial mismanagement or other issues that could pose a reputational risk to ICANN or that suggest heightened risk of misuse of proceeds.

Furthermore, the vendor will have to show a demonstrated understanding of and commitment to ICANN's requirements for transparency and accountability. See: https://www.icann.org/resources/accountability.

# 5 RFP 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.

| Activity | Estimated Dates |
|---|---|
| RFP published | 5 June 2023 |
| **Participants to indicate interest in submitting RFP proposal** | **16 June 2023 by 23:59 UTC** |
| **Participants submit any questions to ICANN** | **20 June 2023 by 23:59 UTC** |
| ICANN responds to participant questions | 27 June 2023 |
| **Participant responses due by** | **7 July 2023 by 23:59 UTC** |
| Evaluation of responses | Through 31 August 2023 |
| Final evaluations, contracting and award | Through 2 October 2023 |

# 6 Terms and Conditions

**General Terms and Conditions**

1. Submission of a proposal shall constitute each 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 the 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.

4. As a requirement for the vendor, we expect that you will comply with all relevant data protection laws and regulations and will have policies and procedures in place to protect the privacy of any personal information that you collect or process on our behalf. You must respect data subjects' right to control their personal information and ensure that their data is kept secure and used only for the purposes for which it was provided. You must never sell, rent, or share personal data you process on our behalf with third parties. We expect that you will take all necessary steps to ensure the security and confidentiality of any personal data that you process on our behalf, including implementing appropriate technical and organizational measures to prevent unauthorized access, use, or disclosure. We also expect you to enter into any necessary additional agreements to ensure data protection. Compliance with these requirements will be a key consideration in our selection of a vendor.

**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 the 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 ten (10) 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, responses to questions related to those requirements, 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.

**Appendix 1: ICANN Service Architecture and Infrastructure Requirements**

ICANN expects the vendor to provide a cloud-based solution to meet ICANN functional requirements. The following are ICANN's service architecture and infrastructure requirements for 3rd party providers.

| **Design Requirement** | **Minimum Requirement Details** | **Benefits of Requirement** |
|---|---|---|
| Backups | Daily incremental, Weekly Full, Retained for 30 days<br>Databases must use transaction logging or another mechanism to permit full recovery<br>Backups should be retrieval via a TLS API or secure file transfer method | Data integrity and Service Availability |
| Local High Availability | No major component should be a single point of failure:<br>• Servers<br>• Data Storage System (local RAID, SAN, NAS, DAS)<br>• Object storage, NoSQL, and Sub/Pub messaging systems<br>• Electric power sources, batteries, and backup power generation<br>• Internet connectivity<br>• Ethernet switching<br>• Local routing which includes a redundant gateway mechanism<br>• Load balancing<br>• Authoritative and caching DNS systems | Service Availability |
| Geographic or Regional High Availability | Due to the projected user population, the service requires geographic or regional high availability to ensure good performance regardless of end user location, available at an ICANN tier 2 level (e.g., 99.995% uptime). | Service Availability |

| | | |
|---|---|---|
| Storage Performance | Low level storage performance requirements should be understood to ensure appropriate block level storage is procured. This is for container, pod, OS level storage needs.<br><br>We do not recommend using a file system as a database mechanism since SQL or NoSQL often scale much better but sometimes storing and retrieving files is key to a system function. | Service Reliability and Performance |
| Network Requirements | A reasonably detailed diagram of inbound and outbound network connections of the service should be supplied.<br>● Ports and protocols in use for connections in and out of the service<br>● Estimated network throughput both in and out of the service<br>● Nature of network traffic: sustained, bursty, or a combination of both<br>● Location of end users<br>● Interfaces that need special firewall rules and VPN access | Corporate Standard<br>Service Reliability and Performance<br>Service Availability |
| Monitoring | Each key infrastructure component is monitored and alerts are sent to appropriate people to respond<br>● Network availability<br>● Storage availability<br>● Data replication functioning as expected (if relevant)<br>● Process availability<br>● Service endpoints functioning as expected | Service Availability |
| Disaster Recovery | Must have a documented and semi-annually tested plan<br>Must have a DR facility that is geographically diverse (at least 200 miles away)<br>Preference should be given to any design that is active-active or active-hot to minimize an outage | Service Availability |
| Sensitive Data in Multi-Tenant Environments | Because sensitive business data is hosted by this service, the provider must be able to demonstrate that data is encrypted using best practices including but not limited to dedicated keys that are managed with standard controls | Data Integrity and Data Privacy |

| | | |
|---|---|---|
| Content Delivery Network (CDN) | Does the service need to make use of a CDN as part of the service design?<br>• How is the CDN used?<br>• What CDN is used if this is a third party service?<br>Internal services are standardized on AWS Cloudfront CDN | Corporate Standard |
| IPv6 | Must have fully functional and provider redundant IPv6 connectivity | Service Availability |
| DNSSEC | Should have DNSSEC signed service names using the ICANN root anchor or a written statement indicating the date of implementation. | Service DNS Integrity |
| Change Controls | Must have some form of change control which includes an ITIL based change management process or a comparable best practice framework. Agile shops may have an automated release management system that includes testing and rollback which may be acceptable depending on the implementation. | Service Configuration Control |
| Access Auditing | Logs must be present to audit who, what, when and from where access was obtained.<br>The logs must be stored in a read-only format and not on the system where access is provided. | Service Access Transparency |
| API | Should have a REST API's for key business functionality and data. | Corporate Standard |
| User Identity Profile | User profiles in applications must be standardized per the ICANN E&IT architectural guideline (e.g., Usernames must support "first.last" or "first.last@icann.org" standard). | Corporate Standard |
| Single Sign On | Applications should support SAML or OpenID (if using SAML should support both SAML SP initiated flow & SAML IDP initiated flow where possible) | Corporate Standard |

| | | |
|---|---|---|
| 2 Factor Authentication | The application or service should support 2 factor authentication. The current 2nd factor used at ICANN is DUO tokens. When Single Sign On is used, like with the Okta portal, the second factor authentication requirement may already be met, but applications with sensitive data should require a second factor upon login even if the user provided 2 factors to authenticate to the Okta portal.<br>• Other second factors, such as certificates or Google tokens, may be acceptable depending on the situation but prior approval is required. | Service Access Security |
| LDAP / Active Directory | If direct LDAP / Active Directory integration is used by the application for authentication or authorization purposes, the user principal value should be "sAMAccount", "userPrincipalName", or "mail" only. Using ICANN AD/LDAP by 3rd party providers for direct authentication purposes is not supported. | Corporate Standard |
| Email | If externally hosted and we want email to be sent from an icann.org address, the vendor must be able to send email from a custom assigned domain name like "@acme.icann.org" | Corporate Standard |
| Service Level Agreement | A service level agreement (SLA) must be provided that includes adequate uptime to meet business requirements and includes penalties for not meeting the target.<br>The SLA should cover all business relevant aspects of the service. | Service Reliability |
| Audit Report | The provider should have an industry recognized operations audit report. The audit needs may vary based on the type of service but the audit must cover essential operational and security controls. | Vendor Process Transparency |