

# **Project Overview for the ICANN New gTLD Program: 2026 Round Background Screening Services Request for Proposal (RFP)**

5 November 2025



---

# 1 Introduction

## 1.1 General Instructions

This document provides an overview of the Request for Proposal (RFP) for Background Screening Services for the New Generic Top-Level Domains (gTLD) Program: 2026 Round (the Program). This RFP overview provides background and pertinent information regarding the requirements for RFP respondents. The RFP comprises this document as well as other documents that are hosted in the ICANN sourcing tool (Jaggaer).

Indications of interest are to be submitted by emailing [2026-round-background-screening-services-rfp@icann.org](mailto:2026-round-background-screening-services-rfp@icann.org) with the following information, upon which access will be provided to the RFP:

1. Name of the organization.
2. Name of the contact.
3. Email address of the contact.

Responses to the RFP should be electronically submitted by **23:59 UTC on 16 January 2026** using ICANN's sourcing tool. Responses to the RFP will not be accepted via other means. ICANN will only accept responses provided in English.

## 1.2 About the Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems. 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](http://www.icann.org) for more information.

## 1.3 About the New Generic Top-Level Domain (gTLD) Program: 2026 Round

The Program is a community-driven initiative that is enabling the continued expansion of the Domain Name System (DNS). Through the introduction of new gTLDs, including domain names in a variety of scripts and languages, the Program aims to encourage innovation, competition, and consumer choice.

Every computer on the Internet has a unique numerical address called an Internet Protocol address. The DNS makes the Internet more 'user-friendly' by allowing users to enter names, rather than having to remember a long string of numbers for the website they wish to visit.

---

Top-level domains (TLDs) form the last part of a domain name, appearing after the dot. For example, in the domain name icann.org, the characters 'org' identify the TLD.

Through the 2012 round of the New gTLD Program, more than 1,200 new unique names like .futbol and .pizza, and names in other alphabets and languages were added to the Internet, which has helped to encourage innovation, competition, and consumer choice in the domain name industry. The Program gives businesses, communities, governments and other organizations the chance to apply for new gTLDs tailored to fit their organization, community, culture, language, and customer interests.

The 2026 round of new gTLDs will offer even more domain names in longer lengths and different scripts. These are an important part of the expansion of the DNS because they allow speakers of non-Latin-based languages to access the Internet using their own language or writing system. The application window for the 2026 round of gTLDs is expected to open in April 2026.

The Program is being implemented by ICANN in line with community-developed policy recommendations contained in the Generic Names Supporting Organization's [Final Report on the new gTLD Subsequent Procedures Policy Development Process](#) ("Final Report").

## 1.4 RFP Objectives

ICANN is seeking to identify a qualified provider to deliver background screening services as part of the application process for the New gTLD Program. The purpose of the RFP is to invite prospective providers to submit proposals for ICANN to evaluate capabilities and expertise. Additionally, ICANN is looking for proposals of the overall costs on a per-evaluation basis.

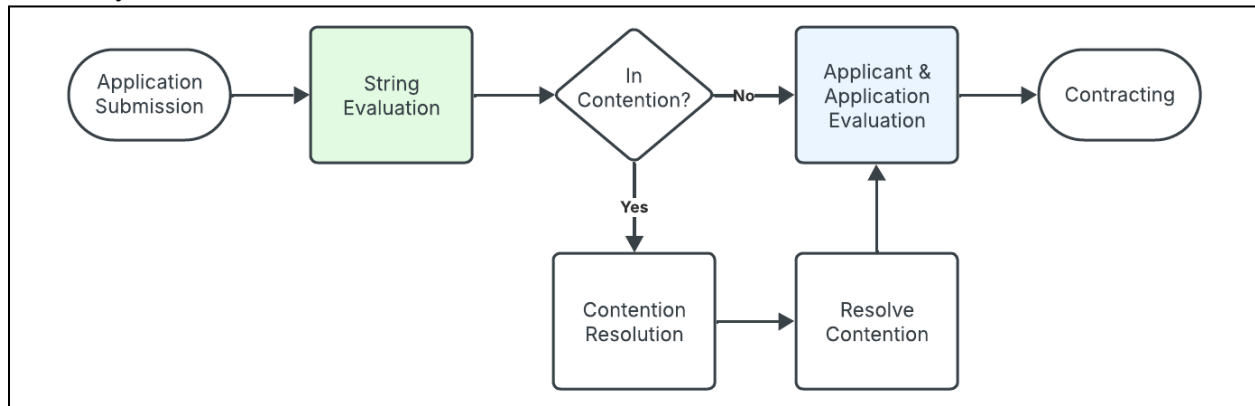
The RFP is public and announced on ICANN's website, and any entity may provide a response.

## 1.5 Background Screening Process

[Background Screening](#) (BGS) is a mandatory component of the New gTLD Program's Applicant Evaluation phase. Its purpose is to safeguard registrants and the public interest by ensuring corporations, organizations, or institutions are in good standing and eligible to operate a gTLD.

Screening will occur within Applicant and Application Evaluation (see Summary of Process Flow below) and consider the organizational information submitted by applicants. Additional screening may be required if an applicant updates key information such as ownership, directors, or officers.

## Summary of Process Flow



As a reference point, the 2012 round received 1,900 applications, representing over 1,100 unique applicants. For the 2026 Round, we are forecasting a need for background screening services for an estimated 800 applicants.

The screening requires the review of organizational and individual information, relevant public records, and the assessment of applicants based on the eligibility criteria outlined in the Applicant Guidebook. Entities that are publicly traded on the world's top 25 stock exchanges may be screened through a modified path that reflects the extensive due diligence and ongoing oversight already conducted by exchanges, regulators, and shareholders.

At the conclusion of the review, the provider will deliver determinations of either Pass/No Issues or Warning/Issues Found, with supporting rationale. ICANN may request clarification or initiate extended evaluation if concerns remain.

## 2 Scope of Work

The Background Screening Provider is expected to manage and conduct evaluations based upon the processes and procedures agreed upon between ICANN and the selected provider.

In accordance with the Applicant Guidebook (AGB) and all applicable ICANN policies, the provider must demonstrate the ability to deliver on the following:

### A. Project Management:

- a. Managing the external evaluation process, including assessing eligibility and qualification requirements, and issuing pass/fail determinations according to the evaluation criteria and agreed upon procedures.
- b. Develop and maintain an Evaluation Guide documenting procedures, definitions, examples and methodology to ensure consistency.
- c. Support ICANN's quality control program and address feedback for process improvement.

### B. Forming and Managing Resources to Assess Applications:

- a. Assemble qualified resources with relevant expertise in legal, compliance, reputation risk, and due diligence.

- 
- b. Train resources on ICANN specific eligibility criteria, clarifying questions and the use of the Evaluation Guide.
  - c. Ensure all resources adhere to conflict of interest policies and confidentiality requirements.
  - d. Maintain continuity of expertise throughout the evaluation cycle.

### **C. Conduct Background Screenings**

- a. Perform screenings on entities and individuals named in applications (including directors, officers, partners, major shareholders, ultimate parent/ control).
- b. Apply differentiated processes for publicly traded corporations listed on the top 25 exchanges (as determined by the World Federation of Exchanges).
- c. Use global sources (sanctions lists, watchlists, media, reputational checks, etc.) to confirm applicant and individuals named within the Organizational Account Record are free and absent of:
  - i. Convictions of any crime related to financial or corporate governance activities, or judgments by a court to have committed fraud or breach of fiduciary duty, or subject of a judicial determination that is the substantive equivalent of any of these within the last ten years.
  - ii. Disciplinary actions by any government or industry regulatory body for conduct involving dishonesty or misuse of funds of others within the last ten years.
  - iii. Convictions of any willful tax-related fraud or willful evasion of tax liabilities within the last ten years.
  - iv. Convictions of perjury, forswearing, failing to cooperate with a law enforcement investigation, or making false statements to a law enforcement agency or representative within the last ten years.
  - v. Convictions of any crime involving the use of computers, telephony systems, telecommunications or the Internet to facilitate the commission of crimes.
  - vi. Convictions of any crime involving the use of a weapon, force, or the threat of force.
  - vii. Convictions of any violent or sexual offense victimizing children, the elderly, or individuals with disabilities.
  - viii. Convictions within the last ten years of the illegal sale, manufacture, or distribution of pharmaceutical drugs, or a conviction or successful extradited for any offense described in Article 3 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.  
Note: A past conviction for an offense that is no longer a criminal offense in the jurisdiction at the time of application shall not be considered.
  - ix. Convictions or been successfully extradited for any offense described in the United Nations Convention against Transnational Organized Crime (all Protocols).
  - x. Convictions of aiding, abetting, facilitating, enabling, conspiring to commit, any of the listed crimes above.
  - xi. Entrance of a guilty plea as part of a plea agreement or having a court case in any jurisdiction with a disposition of Adjudicated Guilty or Adjudication Withheld (or regional equivalents) within the respective timeframes listed above for any of the listed crimes.

- 
- xii. Systematic or repetitive engagement in cybersquatting, as defined in the Uniform Domain Name Dispute Resolution Policy (UDRP), 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 systematic or repetitive engagement in cybersquatting.
  - d. Note, an applicant must answer the following questions concerning the eligibility criteria, ensuring that all information provided complies with applicable laws and regulations. The background screening provider will flag any inconsistencies it finds with the applicant responses/disclosures:
    - i. Confirm to have read and understood the eligibility criteria and declare that neither the applicant nor any individuals named within the Organizational Account Record are subject to any of the above criteria that could impede eligibility.
    - ii. Confirm that neither the applicant nor any of the individuals or entities named within the Organizational Account – whether in their current capacity or as part of a previous entity over which they had ownership or control – have been subject to any decisions indicating involvement in cybersquatting, as defined in the Uniform Domain Name Dispute Resolution Policy (UDRP), Anti-cybersquatting Consumer Protection Act (ACPA), or equivalent legislation. This includes engagement in reverse domain name hijacking under the UDRP or bad faith or reckless disregard under the ACPA or equivalent legislation within the last ten years. If unable to confirm, please provide an explanation. Note related to question 2 above: Three or more such decisions with one occurring in the last four years will generally be considered to constitute a pattern.
      - 1. Confirm that neither the applicant nor any individuals named in the Organizational Account Record – either in their current capacity or as part of a previous entity over which they had ownership or control – has been subject to a final determination by a dispute resolution provider or a court of competent jurisdiction for intellectual property infringement related to registration or use of a domain name within the last ten years. If unable to confirm, please provide an explanation.
      - 2. Confirm that the applicant and individuals or entities named within the Organizational Account – either in their current capacity or as part of a previous entity over which they had ownership or control – have not been subject to a final determination related to the Uniform Rapid Suspension System (URS) Policy or Post-Delegation Dispute Resolution Procedures (PDDRP). If unable to confirm, please provide an explanation.
  - e. Develop and apply Pass/Fail procedures that map directly to the AGB section [6.1.2.1 New gTLD Program Eligibility Criteria](#).
  - f. Prepare Clarifying Questions when data is incomplete or inconsistent, requiring applicant responses within the specified timeframes
  - g. Conduct rescreenings upon ICANN's notification of material changes that occurred (ownership, directors, officers, etc.)

---

#### **D. Managing the Background Screening Program**

- a. Ensure the secure intake and transmission of applicant data.
- b. Deliver results within agreed SLAs for both individual and batch processing.
- c. Conduct calibration exercises across resources (and across providers, if multiple) to ensure consistent application of criteria and determinations.
- d. Support Extended Evaluation requests, including issuing additional clarifying questions or deeper analysis.
- e. Maintain documentation of determinations and rationale for accountability.

#### **E. Managing Conflict of Interest**

- a. Ensuring all internal and/or external resources participating in the evaluation process comply with [AGB Appendix 7](#) for Conflict of Interest and [Appendix 8](#) for Code of Conduct and Conflict of Interest Guidelines for Service Providers, as developed in cooperation with ICANN.

#### **F. Maintaining Document Security**

- a. Complying with all relevant data protection laws and regulations, and establishing policies and procedures to protect the privacy of any personal information that the provider collects or processes on our behalf. The provider 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. The provider must never sell, rent, or share personal data processed on our behalf with third parties. ICANN expects that the provider will take all necessary steps to ensure the security and confidentiality of any personal data that is processed on its behalf.

## **2.1 Scope of Work Timeline**

ICANN anticipates that work on this scope will occur with the Applicant and Application Evaluation phase of the Program, which is expected to start by June or July 2027.

## **2.2 Quality Control**

To assure the community and all applicants that evaluations are objectively conducted and adhere to the processes in the Applicant Guidebook, evaluations and resources work may be reviewed by an independent quality control provider. This provider may request information on how an evaluation (or set of evaluations) was performed and is intended to determine if applications are being evaluated according to the established procedures. The provider may recommend process improvements to ICANN that will be reviewed and may be passed on to resources.

## 2.3 Deliverables

### Infrastructure and Process Setup

Deliverables	Deadline/Milestones
Submit documentation describing methodology, including how it performs screenings, identify results, data sources, escalation protocols, conflicts of interest process and procedures.	Within 45 calendar days of contract execution
Provide ICANN with available options for intake of applicant information to perform screening and reporting of results	Within 45 calendar days of contract execution
Establish and test secure intake and data transmission solution with ICANN, including encryption, file formats, and audit logging	Complete and test before applications assigned
If API is used: Provide endpoint documentation, test credentials, ICANN integration requirements, and implementation timeline	At least 30 calendar days prior to evaluation launch
TLD Application Management System (TAMS) access: Provide a list of individual users that require access to the system to provide determinations and upload result reports.	At least 30 calendar days prior to evaluation launch
If provider is offering access to its portal: Provide login credentials, user roles, audit trail setup, and ICANN user guide for accessing reports	At least 30 calendar days prior to evaluation launch
If file transfer is used: Provide secure folder structure, naming conventions, encryption method, and confirmation process for file submissions	At least 30 calendar days prior to evaluation launch

### Application Screening and Determination

Deliverables	Deadline/Milestones
Conduct screenings on the applying entity including its key individuals and related entities: directors, officers, partners, major shareholders, parent, ultimate parent, and ultimate control (standard and top 25 exchanges). If potential issues are identified, recommend clarifying questions and follow-up actions.	To be defined between ICANN and provider
If notified of an applicant change, complete rescreening within agreed upon SLA	To be defined between ICANN and provider
Review applicable comments from ICANN's Application Comment Forum	Ongoing during evaluation period
Deliver screening report and determination of Pass/No Issues or	To be defined between

Warning/ Issues Found with rationale or identify clarifying questions prior to determinations in alignment with defined service levels	ICANN and provider
--	--------------------

### Resource Management

Deliverables	Deadline/Milestones
Complete ICANN Onboarding and obtain access to TAMS for provider staff	ICANN and Provider will agree on timing; will occur in coordination with Provider onboarding for this phase of the round
Train resources on how to use TAMS, including reviewing application materials, submitting clarifying questions, and uploading evaluation scoring	ICANN and Provider will agree on timing; will occur in coordination with Provider onboarding for this phase of the round
Train resources on eligibility criteria, clarifying questions, use of Evaluation Guide and handling of personal data	ICANN and Provider will agree on timing; will occur in coordination with Provider onboarding for this phase of the round
Maintain and manage conflicts of interest and recusal process for any conflicted parties participating in an evaluation	Ongoing
Identify resources with expertise in legal, compliance, governance, and reputational due diligence to perform evaluations	By start of evaluation period
Manage workload, deadlines, and feedback to ensure consistency across all evaluations	Ongoing
Maintain internal documentation and a knowledge base to ensure consistency across panel rotations and for new panelist onboarding	Ongoing
Facilitate calibration sessions across panelists (and panels if relevant) to align scoring judgements and improve consistency in evaluations	Prior to launch and as needed in evaluation period

### Communications and Reporting

Deliverables	Deadline/Milestones
--------------	---------------------

Track and manage responses to clarifying questions	To be defined between ICANN and provider
Deliver a report for ICANN summarizing outcomes, lessons learned, and recommendations for future rounds of Background Screening	To be defined between ICANN and provider

### Compliance

Deliverables	Deadline/Milestones
Apply documented procedures equally and consistently across all applications	Ongoing
Ensure compliance with global data protection laws and ICANN privacy policy	Ongoing
Adhere to ICANN's Code of Conduct and Conflict of Interest Guidelines for Service Providers	Ongoing
Retain records and reports securely for the period defined by ICANN's data retention policy	As defined by ICANN and provider
Notify ICANN of changes to screening methodology, tool, or jurisdictional requirements	Ongoing
Cooperate with an ICANN-designated Quality Control provider to ensure consistency of evaluations and adherence to documented processes. Respond to ICANN-generated suggestions for process improvements	Ongoing

### Reporting and Technology Interface

Deliverables	Deadline/Milestones
Deliver reports in a secure format through at least one of the following: API, ICANN's TLD application management system, secure portal, file transfer, etc.	Ongoing, mechanism to be agreed upon

### Ongoing Support and Compliance

Deliverables	Deadline/Milestones
Participate in ongoing meetings with ICANN to review flagged applications and clarify any eligibility criteria	To be defined by ICANN and provider
Provide documentation for quality control procedures	By start of evaluation period

---

## 3 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. Experience and Expertise
2. Time and Resources
3. Evaluation and Assessment
4. Resource Management
5. Methodology and Approach
6. Quality Control and Reporting
7. Information Security and Data Privacy
8. Conflict of Interest Management
9. Pricing
10. Reference Checks
11. Financial Health

### 3.1 Key Requirements

The provider must be able to adhere to the complete list of requirements as listed in the Jaggaer Portal. A summary of the key requirements is set out below:

1. Provider must be a well established firm or organization with significant demonstrated expertise in conducting background screenings of corporations, organizations, individuals, and institutions. Such expertise will include:
  - a. Experience in conducting legal, financial, and reputational checks across multiple jurisdictions
  - b. Ability to manage global investigations consistently and objectively.
  - c. Experience developing systematic approaches for verifying applicant provided information and public comments
2. The provider must have the ability to manage evaluation processes of international projects and organizations.
3. Provider must have a demonstrated ability to develop work methods, evaluation/assessment approaches and reporting based on specific objectives and criteria.
4. Ability to design and manage end-to-end screening workflows, including applicant intake, clarifying questions, and final determinations.
5. Ability to convene and manage qualified resources with relevant expertise (e.g. financial, due diligence, governance, compliance).

6. The provider must receive ICANN's approval before engaging any third-party firms / independent contractors (i.e., firms/contractors with whom you propose to subcontract) related to this project.
7. The provider must have the ability to maintain data security and integrity of the process, including by incorporating the principles of privacy and security by design into their work, to help ensure that privacy and security are considered throughout the project lifecycle, and that personal data is processed in a secure and compliant manner.
8. All Providers must demonstrate a robust conflict of interest policy for the resources in place. Eligibility to serve as a background screening provider will be based on an assessment of potential conflicts of interest. Should any applicants submit applications that would present a conflict of interest, the provider must have an established process for recusal and provide an alternative evaluation panelist within a reasonable timeframe. Please refer to the AGB [Appendix 7](#) for Conflict of Interest and [Appendix 8](#) for Code of Conduct and Conflict of Interest Guidelines for Service Providers which apply to Evaluation Resources.
9. The provider must support ICANN in addressing any accountability mechanisms described in the AGB for evaluation results and to supply necessary information and documentation to ICANN, as needed, on an ongoing basis.
10. The provider and all employees and/or subcontractors are expected to complete ICANN-led provider onboarding prior to engaging in the contracted effort. This will include information on ICANN, its mission, the New gTLD Program: 2026 Round as well as any system and process training ICANN deems necessary. ICANN will do its best to contain training to material relevant for the provider's contracted work. ICANN expects this to occur prior to the start of provider's work.
11. The provider must give ICANN pricing on a per-application-evaluated basis. ICANN wants to understand the aspects of each respondent's pricing. Provider should include all components of their pricing in the pricing worksheet as discrete line items for ICANN's evaluation purposes. Final pricing for this work will be stated in an executed agreement on a per-evaluation price, which includes the price for the evaluations and any other accepted pricing components.
12. ICANN requires the provider to obtain reference checks. Providers should have relevant references available for ICANN to contact.

## 4 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 November 2025
<b>Participants submit any questions to ICANN via Jaggaer Q&amp;A Board</b>	<b>24 November 2025 by 23:59 UTC</b>
ICANN responds to participant questions	15 December 2025

<b>Participant proposals due by</b>	<b>16 January 2026 by 23:59 UTC</b>
ICANN reviews proposals	Q1 2026
Final evaluations, contracting and award	Q2 2026

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

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 respondent does not want ICANN to disclose or use other than for the purposes of evaluating the proposal, that information should be marked with appropriate confidentiality markings.

3. As a requirement for the provider, ICANN expects that respondent 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 respondent collects or processes on behalf of ICANN. Respondent 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. Respondent must never sell, rent, or share personal data they process on ICANN's behalf with third parties. ICANN expects that respondent will take all necessary steps to ensure the security and confidentiality of any personal data that they process on behalf of ICANN, including implementing appropriate technical and organizational measures to prevent unauthorized access, use, or disclosure. Compliance with these requirements will be a key consideration in the selection of a provider.

### Discrepancies, Omissions and Additional Information

1. Respondent is responsible for examining the 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 the RFP, respondent must notify ICANN of such findings immediately in writing via email no later than 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 staff members, agents, or representatives concerning the RFP. If respondent requires additional information, respondent must request that the issuer of the 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 the RFP will be provided to all prospective respondents receiving the RFP. All supplemental information issued by ICANN will form part of the 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 the 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 the 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 the 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 the 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.