Registry Service Provider Evaluation Handbook

This document describes the application submission process for Registry Service Providers (RSPs). Users will provide information within the application system, and the data will be administratively reviewed, prioritized, and published.

January 2024
Version 1.0

TABLE OF CONTENTS

Document Meta-Data:

- This document will be published both as a stand-alone handbook and as a module of the larger Applicant Support Guidebook.
- Content highlighted in bright yellow covers material that needs review and/or has yet to be determined.

Document History:

Revision Description	Initial Version	**Date**	September 2023
	First IRT Version		January 2024

[This page should be deleted before publication.]

1. Introduction

This handbook provides an overview of the application process to become an evaluated Registry Service Provider (RSP) as part of the New gTLD Program: Next Round ("Next Round").

RSPs play an important role in the Domain Name System (DNS) eco-system, including supporting technical operations and providing services to registry operators (ROs) for top-level domains (TLDs), and RSPs are an important component of Next Round applications for new gTLDs. As part of the overall Next Round gTLD application process, ROs must identify an evaluated RSP that will provide support for all the critical registry functions[1].

The RSP Evaluation Program provides for testing and evaluation of an RSP to ensure it meets certain technical and operational requirements to provide technical services to ROs and allows a successfully evaluated RSP to then be identified by an RO applicant in the Next Round.

Note that ROs can provide their own technical operations or outsource certain technical operations to third-party providers. Regardless of the organization providing these technical operations, the entities providing such operations are referred to as RSPs. When ROs outsource technical operations to third-party RSPs, this may help ROs to reduce costs, improve efficiency, and focus on core business activities.

The RSP Evaluation Program is offering the option for an RSP to become pre-evaluated prior to the opening of Next Round new gTLD applications. Opting to undergo the RSP evaluation before the opening of new gTLD applications may reduce the overhead and time necessary to complete a new gTLD application. Alternatively, an RSP may also be evaluated during an RO's new gTLD application if it has been selected by the RO but did not opt to become pre-evaluated.

Please note that the RSP Evaluation Program is not a certification program. The Program provides an evaluation at a specific point in time of potential RSPs based on the criteria developed by ICANN in consultation with the community. It is the responsibility of New gTLD applicants who plan to outsource certain technical operations to an RSP(s) to do its own diligence to ensure it would like to engage the services of a particular RSP.

1.1. Updates to the RSP Handbook

This handbook forms the basis of the RSP Evaluation Program. ICANN org reserves the right to make reasonable updates and changes to the handbook at any time, including as the possible

[1] Defined in Paragraph 6.1 of Specification 10 of the Registry Agreement as DNS, DNSSEC, EPP, RDAP, and Data Escrow.

result of new technical standards, reference documents, or policies that might be adopted during the course of the application process. Any such updates or revisions will be posted on ICANN's website (TBD_URL).

1.2. Questions About the RSP Evaluation Program

For general questions about the RSP Evaluation program, an end-user should use the customer support resources available via ICANN Global Support.

Before using the RSP Portal, applicants may seek clarification about any aspect of the RSP Evaluation Program by sending email to globalsupport@icann.org. Applicants who are unsure of the requirements needed to successfully pass RSP evaluation are encouraged to seek clarifying information before using the RSP Portal.

For assistance and questions an applicant may have during the process of completing the evaluation, applicants should use the RSP Portal. Applicants who are unsure of the information being sought in a question or the parameters for acceptable documentation are encouraged to communicate these questions through the RSP Portal. This helps to reduce the number of clarifying questions with evaluators, which could potentially impact the time frame associated with application processing.

ICANN org will not grant applicant requests for in-person, telephone, or video consultations regarding the preparation of an application.

Answers to inquiries will only provide clarification about the application and procedures. ICANN org will not provide consulting, financial, or legal advice.

1.3. Types of RSP

There are multiple types of RSPs, each delivering a set of unique functions necessary for the operation of a gTLD. An organization can fulfill one or more of these functions, and must separately apply for each type of RSP they intend to fulfill. At a minimum, the operations necessary to operate a gTLD are provided by a Main RSP, a DNSSEC RSP, and one or more DNS RSPs.

1.3.1. Main RSP

A Main RSP is responsible for the registrations of domain names and the reporting functions associated with domain registration. A Main RSP will operate a domain registration database, conduct data escrow and reporting operations regarding those registrations, operate Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) services, and conduct other functions as required by ICANN.

Main RSPs may offer to support additional Registry Services that ROs are authorized by ICANN to provide of the nature found in Exhibit A of the Registry Agreements of several gTLDs currently delegated. Registry Services offered by an RSP must be approved by ICANN org. Main RSPs are automatically approved to offer Registry Services categorized as Fast Track when the pre-approved default Registry Agreement amendment language is used. All other Registry Services require evaluation before approval by ICANN org; evaluation of those Registry Services may incur additional fees.

1.3.2. DNSSEC RSP

A DNSSEC RSP operates the cryptographic functions necessary for the Domain Name System Security Extensions (DNSSEC) of a gTLD. These functions include the maintenance and safe-handling of cryptographic materials, and the cryptographic signing of DNS zone data.

1.3.3. DNS RSP

A DNS RSP operates authoritative DNS servers for a gTLD. This function typically entails the deployment of multiple DNS servers around the world, usually using IP anycast, to serve the domains of a gTLD. An RO may use more than one DNS RSP in order to provide additional resilience, but each RSP used by an RO for this purpose must be evaluated.

1.3.4. Proxy RSP

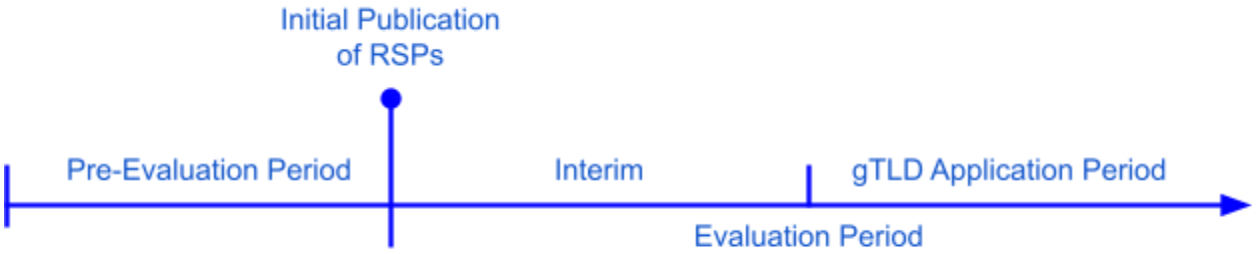
Some ROs may perform registration validation to comply with applicable local law in a given jurisdiction, which is an optional Registry Service required to be approved by ICANN. In some cases, an RO may want to perform this registration validation service through a Proxy RSP. In addition to performing the validation service, the Proxy RSP also ensures that any infrastructure deployed in that jurisdiction operates in accordance with the relevant specifications from the Registry Agreement.

2. Program Timelines

2.1. Evaluation Periods

RSPs may be evaluated in a pre-evaluation period before the Next Round application submission period opens for gTLD applications.

RSPs that have not sought evaluation during the pre-evaluation period must be evaluated during the gTLD application period. The evaluation criteria and testing will be the same as that which occurs during the RSP pre-evaluation period.



RSP Evaluation Program Timeline

The RSP pre-evaluation period will begin approximately 18 months prior to the opening of the submission period for Next Round gTLD applications. This will allow RSP applicants time to complete the process and be published on a publicly available list of RSPs that have successfully passed evaluation.

2.2. Application Submission Dates

ICANN org plans to open the application submission period for RSP Pre-Evaluation on [TBD_Date]. ICANN org plans to close this submission period on [TBD_Date]. ICANN org plans to evaluate applications immediately after the close of the submission period. It is anticipated that RSP evaluations for the Pre-Evaluation phase will conclude on [TBD_Date].

RSPs that are not evaluated during the pre-evaluation phase must seek evaluation during the Next Round gTLD application submission period and may be selected by ROs upon successful evaluation. RSPs that pass evaluation after the RSP Pre-Evaluation Phase will be added to the public list of evaluated RSPs.

2.3. List of Evaluated RSPs

ICANN org plans to publicly list RSPs that have passed evaluation during the pre-evaluation phase on [TBD_Date], subject to the Service Level Target for the public RSP list (see 4.3. Service Level Targets).

Publicly listed RSPs will have obligations to maintain current information with ICANN org including contact information, capacity of their infrastructure, management of pre-approved services, and any other information that may be required in their role as an RSP. RSPs must use the RSP Portal to communicate this information to ICANN org. RSPs failing to meet these obligations will be removed from this list.

3. Information for All Applicants

3.1. Eligibility

Established corporations, organizations, or institutions that are not in breach of agreements with ICANN may submit an RSP application. Applications from individuals or sole proprietorships will not be considered. Applications from or on behalf of yet-to-be-formed legal entities, or applications presupposing the future formation of a legal entity (for example, a pending joint venture) will not be considered.

The RSP Portal requires applicants to provide information on the legal establishment of the applying entity, as well as to identify directors, officers, partners, persons of significant influence, and major shareholders of that entity.

Background screening at both the entity level and the individual level will be conducted for all applicants to confirm eligibility. This inquiry is conducted on the basis of the information provided by the applicant. ICANN org may take into account information received from any source if it is relevant to the criteria in this section. If requested by ICANN org, all applicants will be required to obtain and deliver to ICANN org and ICANN org's background screening vendor any consents or agreements of the entities and/or individuals named in the application form necessary to conduct background screening activities.

In the absence of exceptional circumstances, as determined by ICANN org in its sole discretion, applications from any entity with or including any individual with convictions or decisions of the types listed in (a) – (q) below will be automatically disqualified from the program.

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 ICANN org deems as the substantive equivalent of any of 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 the threat of force;
g. Has ever been convicted of 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 or 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)4,5;
j. Has been convicted, within the respective timeframes, of aiding, abetting, facilitating, enabling, conspiring to commit, or failing to report any of the listed crimes above (i.e., within the past 10 years for crimes listed in (a) - (d) above, or ever for the crimes listed in (e) – (i) above);
k. Has entered a guilty plea as part of a plea agreement or has 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 (i.e., within the past 10 years for crimes listed in (a) – (d) above, or ever for the crimes listed in (e) – (i) above);
l. Is the subject of a disqualification imposed by ICANN and in effect at the time the application is considered;
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 Domain Name Dispute Resolution Policy (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 other 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 been involved in a pattern of adverse, final decisions indicating that the applicant or individual named in the application was engaged in DNS abuse as defined as malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed here). Three or more such decisions with one occurring in the last four years will generally be considered to constitute a pattern.
o. Fails to provide ICANN org with the identifying information necessary to confirm identity at the time of application or to resolve questions of identity during the background screening process;
p. Fails to provide a good faith effort to disclose all relevant information relating to items (a) – (n).
q. Is in breach of agreements with ICANN.

Background screening is in place to protect the public interest in the allocation of critical Internet resources, and ICANN org reserves the right to deny an otherwise qualified application based on any information identified during the background screening process. For example, a final and legally binding decision obtained by a 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 may cause an application to be rejected. ICANN org may also contact the applicant with additional questions based on information obtained in the background screening process.

All applicants are required to provide complete and detailed explanations regarding any of the above events as part of the application. Background screening information will not be made publicly available by ICANN.

Separate from background screening, each applicant will also undergo a legal compliance check as described in Section 4.1.4. Legal Compliance.

3.2. Required Documents

All applicants should be prepared to submit documentation of the applicant's establishment as a specific type of entity in accordance with the applicable laws of its jurisdiction.

As indicated in the relevant questions, supporting documentation should be submitted in the original language. English translations are encouraged.

All documents must be valid at the time of submission.

3.3. Terms and Conditions and Terms of Use

All applicants must agree to a set of Terms and Conditions for the application process. The Terms and Conditions are available in this handbook. Additionally, each user of the RSP Portal and/or the RST System must agree to a Terms of Use in the RSP Portal.

3.4. Data Privacy

Any Personal Information, as defined in the ICANN Privacy Policy, collected, used, or submitted in connection with the RSP Evaluation Program and/or RST will be processed only for lawful purposes and consistent with the purposes for which it was collected. Such Personal Information will be processed in accordance with the New gTLD Program Privacy Statement [TBD_URL] and ICANN Privacy Policy.

3.5. Publication of Applications

Portions of all RSP applications, IDN Services applications, and Registry Services applications will be made public on the published list of evaluated RSPs at the time of publication. RSP application information that will be made public includes responses to select and specific technical questions. ICANN org will not publish personal data of RSP applicants.

3.6. Notice of Changes to Information

If at any time during the evaluation process information previously submitted by an applicant becomes untrue or inaccurate, the applicant must promptly notify ICANN org via the RSP Portal. This includes but is not limited to applicant-specific information including changes in financial position and changes in ownership or control of the applicant, technical information about the applicant's RSP services, past performance, and security certifications.

ICANN org reserves the right to require a re-evaluation of the application in the event of a material change. This could involve additional fees.

Failure to notify ICANN org of any change in circumstances that would render any information provided in the application false or misleading may result in denial of the application.

4. Submitting an Application

Applicants must complete the application form and submit supporting documents using ICANN's RSP Portal. To access the system, each applicant must first register as an RSP Portal user.

The RSP Portal gives applicants the ability to provide required information regarding the applying entity and responses to application questions, and to submit supporting documentation as attachments. Restrictions on the size of responses and the size of attachments as well as the file formats are included in the instructions on the RSP Portal.

All responses to technical questions, including questions regarding the technical aspects of Internationalized Domain Name (IDN) services and questions regarding additional Registry Services, must be submitted in English.

ICANN org will not accept application forms or supporting materials submitted through means other than the RSP Portal (e.g., hard copy, fax, email), unless such submission is in accordance with specific instructions from ICANN org to applicants.

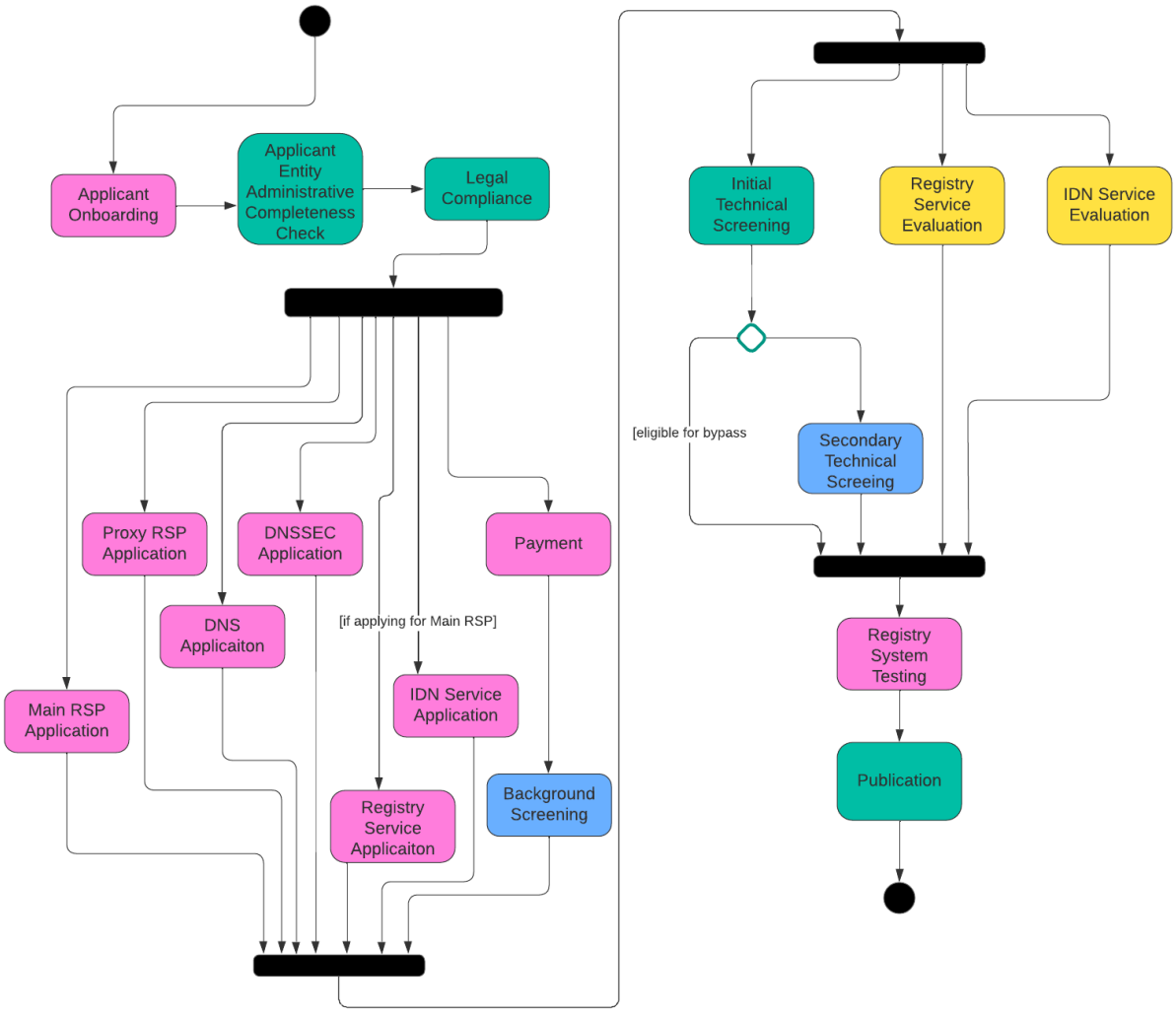
The RSP Portal will be accessible from the SOME_WEBPAGE (TBD_URL) upon agreement to Terms of Use for the RSP Portal and the RST System. RSP Portal users will be required to first

create an ICANN account, if they do not already have one, at https://account.icann.org/ in order to enter into and use the RSP Portal.

4.1. Evaluation Processing Steps

Progression of the RSP Evaluation Process

Evaluation of an RSP has several sequential stages, where advancement to the next stage is dependent on the successful completion of a previous stage. Upon submission of an application, each application will receive an initial technical screening, followed by a secondary technical screening, as described in detail below. However, some applications may be eligible to bypass secondary technical screening.



4.1.1. User Registration

Usage of the RSP Portal is available to the public. All users will be required to first create an ICANN account at https://account.icann.org. The user's ICANN account credentials are used to enter into the RSP Portal.

4.1.2. Applicant Onboarding

Before applying to be an RSP, users will be required to onboard their applicant organization. Each applicant organization must have a minimum of two users registered in the RSP Portal, and may have as many as five users. Two of the users are to be "primary" users with the authority to invite other users of the organization to register and use the RSP Portal.

Only one user may enter an RSP application, Registry Services application, or Internationalized Domain Name (IDN) Service application, and that user will be the main point of contact for that application. Applications can be reassigned among users of the organization. Multiple applications may be completed and submitted concurrently by separate users.

Information collected about the applicant organization includes data specifically about the organization and named individuals with significant influence over the organization such as key executives and stakeholders. This information is used to conduct checks and background screening of the organization, conduct the evaluation of the RSP, and publish the RSP information on the RSP list upon successful evaluation.

Additionally, each applicant organization must name and provide the information of a signatory officer. The signatory officer is an individual designated by the organization to issue payments by the organization to ICANN.

Neither the signatory officer nor any of the key personnel, such as executives and stakeholders, are required to be registered users of the RSP Portal.

Applicant onboarding does not require all information to be given in one sitting. Users will be able to save and provide information at their own pace. However, once the applicant information has been submitted, applicant information can only be changed through the Change Request process.

4.1.3. Completeness Check

ICANN org will conduct an administrative completeness check on submitted organizational profiles. Administrative completeness consists of a review to ensure that all required organizational and user information is legible and complete, mandatory questions are answered, and required supporting documents have been provided.

4.1.4. Legal Compliance

ICANN must comply with all U.S. laws, rules, and regulations. One such set of regulations is the economic and trade sanctions program administered by the Office of Foreign Assets Control (OFAC) of the U.S.Department of the Treasury. These sanctions have been imposed on certain countries, as well as individuals and entities that appear on OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List). ICANN is prohibited from providing most goods or services to residents of sanctioned countries or their governmental entities or to SDNs without an applicable U.S. government authorization or exemption. ICANN generally will not seek a license to provide goods or services to an individual or entity on the SDN List. In the past, when ICANN has been requested to provide services to individuals or entities that are not

SDNs, but are residents of sanctioned countries, ICANN has sought and been granted licenses as required. In any given case, however, OFAC could decide not to issue a requested license.

Each applicant organization and all associated contacts and users of the organization entered into the RSP Portal during applicant onboarding will be checked against the SDN List. If an applicant organization or any of its users or contacts are listed on the SDN List, the applicant organization will be unable to proceed unless ICANN receives a license from OFAC.

4.1.5. Payment

Applicants clearing Legal Compliance will receive instructions on how to submit payment for the fee for the RSP evaluation.

Applicants will be allowed to enter application information in the RSP Portal before payment is received by ICANN org. However, applicants will be unable to submit any applications until payment is received and background screening of the organization has been completed.

Applicants will be notified upon receipt of payment.

Organizations are not required to have an operational RSP at this stage of the evaluation. It will be necessary, however, for an organization to demonstrate a clear understanding of the key technical and operational aspects of an RSP and that it has accomplished some of the groundwork involved.

4.1.6. Background Screening

Background screening will begin after payment of fees. The background screening evaluates the identities of the organization and the individuals named as part of the organization can be against the criteria for eligibility described in Section 3.1. Eligibility.

ICANN org will submit identifying information for the entity, officers, directors, and major shareholders to an international background screening service. The service provider(s) will use the criteria listed in Section 3.1. Eligibility and return results that match these criteria. Only publicly available information will be used in this inquiry.

Note that the applicant is expected to disclose potential problems in meeting the criteria for eligibility, and provide any clarification or explanation at the time of applicant onboarding. Results returned from the background screening process will be matched with the disclosures provided by the applicant; those cases will be followed up to resolve issues of discrepancies or potential false positives.

4.1.7. Technical Questionnaire

A separate technical questionnaire will be available for each RSP application, and the form will vary depending on the type of RSP being applied for. Users will be provided a means to answer application questions at their own pace, and save answers to questions as needed.

Users will not be required to provide answers to each question of a technical questionnaire in one sitting. However, once the technical questionnaire has been submitted, it can only be changed through the Change Request process.

Answers to all technical questions and all supporting documentation submitted as attachments must be in English.

Each question of the technical questionnaire is scored on a pass/fail basis. Many questions will require applicants to provide descriptions of processes or technical mechanisms. Answers that adequately address the content of the questions will be evaluated as a pass.

The RSP questions may be found in Appendix A. RSP Application Technical Questions.

4.1.8. Initial Technical Screening

ICANN org will conduct an initial technical screening on submitted applications only after an applicant passes background screening. This screening consists of a review to ensure that:

- All mandatory questions are answered;
- Required supporting documents are provided in the proper format(s); and
- All answers are reviewed for appropriateness.

Application responses will be reviewed to ensure they are complete and relevant to the information being sought for the type of RSP application being submitted. ICANN org will denote responses that are incomplete or irrelevant; notify applicants of any issues; and provide applicants a limited period of time in which to address them. The application will not proceed until the applicant makes corrections.

4.1.9. Secondary Technical Screening

Responses provided by the applicant to the technical questionnaire may be reviewed by a third-party technical panel to determine whether the applicant is technically qualified and operationally capable of managing an RSP.

If the third-party technical panels have a conflict of interest, the panel(s) cannot proceed with the evaluation. In such a situation, ICANN org will act as the technical panel for secondary technical screening.

During this stage, technical evaluators may seek clarifications from applicants to information submitted by applicants. Applicants will be given two weeks to respond to any clarifications being sought.

Applicants currently operating an RSP for an active gTLD may be eligible to bypass the secondary technical screening. To be eligible, applicants must:

- currently provide service for an active gTLD as the type of RSP under application; and
- have had no service disruptions to any gTLDs for which it provides relevant services reaching the emergency threshold, as defined by Specification 10 of the base new gTLD Registry Agreement, in the six months immediately preceding the submission of the application.

ICANN org will determine eligibility for bypassing the secondary technical screening after submission of each RSP application.

4.1.10. Registry System Testing

For each RSP application and IDN Service applications, applicants will proceed to Registry System Testing (RST) upon successful completion of technical screening(s). This testing requires applicants to demonstrate the capacity to operate a functional RSP. Applicants must pass RST for each type of RSP application and IDN service to complete an evaluation.

Applicants will provide, via the RSP Portal, onboarding data for the Registry System Test (RST) system. At that time, a test request will be provisioned in the RST system according to the RSP application type. Applicants will then be able to conduct technical testing at their own pace via the RST Application Programming Interface (RST-API). RSPs may run tests multiple times if necessary. However, completion of RST requires a final passing run of all RST tests.

Applicants will have access to an escalation process during RST. This escalation process may be used by applicants to receive clarification of test results or to seek adjustment to tests that may be incorrect.

See Section 7. Registry System Testing (RST) for more details.

4.1.11. Registry Services Evaluation

Applicants applying to be a Main RSP will be able to apply to be evaluated to provide additional Registry Services. These additional Registry Services would be included in Exhibit A of the

Registry Agreement for registries supported by the Main RSP. Registry Services may be added to an application in two ways:

1. **Simplified Registry Services Evaluation:** If the applicant is currently serving as an RSP for a gTLD and wishes to offer a Registry Service currently being offered to a gTLD, the applicant can provide:
    a. The name of the Registry Service,
    b. The TLDs in which the Registry Service is offered, and
    c. A description of the Registry Service. The description of the Registry Service should not materially deviate from the contractual language used in the given TLDs.

    Upon submission, these Registry Services will be evaluated.

2. **Full Registry Services Evaluation:** ICANN org will evaluate the service using the principles of the RSEP Policy for Registry Services that are not eligible for simplified registry service evaluation. Upon submission, these Registry Services will be evaluated.

All Main RSP applicants are automatically pre-approved to offer all Fast Track Registry Services with the default, pre-approved Registry Agreement Amendment language. If an RSP is not planning to implement the service in a way that a Registry Operator could use the pre-approved Registry Agreement Amendment language for a Fast Track Registry Service, they must apply for a Registry Service as described above.

Registry Services applications will be evaluated by ICANN org in parallel to the processing of the Main RSP application.

Applicants may apply for more than one Registry Service, and applicants may apply for additional Registry Services through the RSP Portal after having been successfully evaluated as a Main RSP.

The Registry Services questions may be found in Appendix C. Registry Services Application Questions.

4.1.12. Internationalized Domain Name (IDN) Evaluation

A Main RSP may apply to support IDN services based on support for variant TLDs and support for variant IDNs in the second-level.

Each IDN Service application will require the applicant to answer an IDN technical questionnaire and provide, at a minimum, the IDN table for the IDN Service. All IDN service technical questions will be evaluated on a pass/fail basis. Questions will require applicants to provide

documentation of or otherwise describe the technical aspects of IDN services. Answers to questions that materially cover the subject matter will be graded as a pass.

IDN services are denoted by three support levels:

Level 1	IDNs offered at the second-level will have no variant management.
Level 2	The RSP may manage variant IDNs in the second-level and will not support variant TLDs.
Level 3	The RSP may manage variant IDNs in the second-level and may support variant TLDs.

An applicant will only be allowed to select one IDN support level, and applicants will be required to select IDN language/script pairs from a pre-defined catalog. The catalog contains all languages/scripts covered in Second-Level Reference Label Generation Rules (LGR) and languages covered by the Root Zone Label Generation Rules. For all other languages and scripts, ROs will be able to apply for these usages through the IDN Service request upon execution of the Registry Agreement. For each language/script pair selected not using a Second-Level Reference LGR, applicants will be required to upload an applicable IDN table in RFC 7940 format.

IDN applications will be evaluated by ICANN org in parallel to the processing of the Main RSP application.

Applicants may apply for more than one IDN service, and applicants may apply for additional IDN services through the RSP Portal after having been successfully evaluated as a Main RSP.

IDN Service questions may be found in Appendix B. IDN Services Application Technical Questions.

4.2. Customer Service During the Application Process

Assistance will be available to applicants through the RSP Portal. Should users or applicants be unable to use the RSP Portal, assistance may also be sought through ICANN Global Support.

4.3. Service Level Targets

ICANN org commits to the following service level targets (SLTs) during the RSP evaluation process. Each SLT is expressed using the unit “business day”, which is defined as any day of

the week (Monday through Friday) excluding standard US holidays and a week during the holiday season at the end of the year.

Process	SLT
Applicant Completeness Check	TBD
Background Screening	TBD
Initial Technical Screening	TBD
Secondary Technical Screening	TBD
Registry System Testing	N/A
ICANN org Response to Inquiries	TBD
Registry Services Evaluation	TBD
IDN Service Evaluation	TBD
Publication of Evaluated RSP	TBD
Change Request	TBD
[Limited Challenge / Appeal Mechanism]	TBD

4.4. Backup Application Process

If the RSP Portal is unavailable for a period of time that would prevent an applicant from submitting a completed application on time, ICANN org will provide alternative instructions for submitting applications.

5. Fees and Payments

This section describes the fees to be paid by the applicant as well as payment instructions.

5.1. RSP Evaluation Fee

The RSP evaluation fee is required from all applications in the RSP Evaluation Program. This fee is in the amount of USD [TBD_RSP_EVALUATION_FEE]. This fee will be payable to ICANN only via bank wire transfer. Users will be able to begin the RSP application process and enter information into the technical questionnaires before payment is received, but the applicant will

be unable to submit any applications until payment is received. ICANN org will not begin its evaluation of an application unless it has received the full evaluation fee.

The evaluation fee is set to recover costs associated with the program. The fee is set to ensure that the program is fully funded and revenue-neutral and is not subsidized by existing contributions from ICANN funding sources, including generic TLD registries and registrars, ccTLD contributions, and Regional Internet Registry (RIR) contributions.

The evaluation fee covers all required reviews, evaluations, and testing. If a Registry Service application requires the evaluation by a third-party panel, an additional fee will be incurred for this review. See 5.2. Potential Additional Fees Required.

An applicant that wishes to withdraw an application must initiate the process through the RSP Portal. Withdrawal of an application is final and irrevocable. In the case of withdrawal, no refunds on the RSP evaluation fee will be issued.

5.2. Potential Additional Fees Required

If applicable, the Registry Services review fee is payable for additional costs incurred in referring an application to a third-party panel for an extended technical review. This review is separate from a third-party review done in the Secondary Technical Screening for an RSP application. Applicants will be notified if a Registry Service application will require third-party panel evaluation. The fee for third-party panel evaluation is anticipated to be USD [TBD_FEES_REQUIRED_FOR_RSTEP]. ˜In every case, the applicant will be advised of the cost before initiation of the review.

5.3. Payment Methods

Payments to ICANN must be submitted by wire transfer. Instructions for making a payment by wire transfer will be available in the RSP Portal.

5.4. Applicant’s Withdrawal of an Application

Applicants may withdraw their application at any time during the application process. Applicants submitting an application after having withdrawn a previous application will be required to pay the same processing fee and proceed through the process as a new application.

6. Parties Involved in Evaluation

A number of independent experts and groups play a part in performing various reviews in the evaluation process. A brief description of the various panels, their evaluation roles, and the circumstances under which they work is included in this section.

6.1. Panels and Roles

Members of all panels are required to abide by an established Code of Conduct and Conflict of Interest guidelines.

6.1.1. Third-Party Technical Evaluation Panel

The third-Party technical evaluation panel will review the technical components of each RSP application, subject to the criteria for by-passing secondary technical screening, against the criteria in this handbook in order to determine whether the applicant is technically and operationally capable of operating and performing the functions of an RSP.

6.1.2. Registry Services Third-Party Panel

The registry services third-party panel will review proposed registry services in the application to determine if they pose a risk of a meaningful adverse impact on security or stability.

6.2. Panel Selection Process

Based on an extensive selection process, ICANN org has selected qualified third-party providers to perform the various reviews. In addition to the specific subject matter expertise required for each panel, special qualifications are required, including:

- The ability to convene – or have the capacity to convene - globally diverse panels and to evaluate applications from all regions of the world.
- Familiarity with the IETF IDNA standards, Unicode standards, relevant RFCs, and the terminology associated with IDNs.
- Experience with the relevant standards used when providing the following services: DNS, EPP, RDAP, DNSSEC, and Data Escrow.
- The ability to scale quickly to meet the demands of the evaluation of an unknown number of applications. At present, it is not known how many applications will be received, how complex they will be, nor whether they will be predominantly for Main RSPs or other types.
- The ability to evaluate applications within the required time frames of secondary technical screening.

6.3. Code of Conduct Guidelines for Panelists

The purpose of the RSP Program Code of Conduct is to ensure that panelists adhere to the highest ethical standards.

Panelists shall conduct themselves as thoughtful, competent, well prepared, and impartial professionals throughout the application process. Panelists are expected to comply with equity

and high ethical standards while assuring the Internet community, its constituents, and the public of objectivity, integrity, confidentiality, and credibility. Unethical actions, or even the appearance of compromise, are not acceptable. Panelists are expected to be guided by the following principles in carrying out their respective responsibilities. This code is intended to summarize the principles and nothing in this code should be considered as limiting the duties, obligations, or legal requirements with which panelists must comply.

Bias -- Panelists shall:

- Not advance personal agendas or non-ICANN approved agendas in the evaluation of applications;
- Examine facts as they exist and not be influenced by past reputation, media accounts, or unverified statements about the applications being evaluated;
- Exclude themselves from participating in the evaluation of an application if, to their knowledge, there is some predisposing factor that could prejudice them with respect to such evaluation; and
- Exclude themselves from evaluation activities if they are philosophically opposed to or are on record as having made a general criticism about a specific type of applicant or application.

Compensation/Gifts -- Panelists shall not request or accept any compensation whatsoever or any gifts of substance from the applicant being reviewed or anyone affiliated with the applicant. (Gifts of substance would include any gift greater than US$25 in value).

If the giving of small tokens is important to the applicant's culture, panelists may accept these tokens; however, the total of such tokens must not exceed US$25 in value. If in doubt, the panelist should err on the side of caution by declining gifts of any kind.

Conflicts of Interest -- Panelists shall act in accordance with the "RSP Evaluation Program Conflicts of Interest Guidelines" (see below).

Confidentiality -- Confidentiality is an integral part of the evaluation process. Panelists must have access to sensitive information in order to conduct evaluations. Panelists must maintain confidentiality of information entrusted to them by ICANN and the applicant and any other confidential information provided to them from whatever source, except when disclosure is legally mandated or has been authorized by ICANN. "Confidential information" includes all elements of the program and information gathered as part of the process – which includes but is not limited to documents, interviews, discussions, interpretations, and analyses – related to the review of any RSP application.

Affirmation -- All Panelists shall read this code prior to commencing evaluation services and shall certify in writing that they have read and understand the code.

6.3.1. Conflict of Interest Guidelines for Panelists

It is recognized that third-party providers may have a large number of employees in several countries serving numerous clients. In fact, it is possible that a number of panelists may be very well known within the registry/registrar community and have provided professional services to a number of potential applicants.

To safeguard against the potential for inappropriate influence and ensure applications are evaluated in an objective and independent manner, free from any actual, potential, or perceived conflicts of interest, ICANN has established detailed Conflict of Interest guidelines and procedures that will be followed by the evaluation panelists. To help ensure that the guidelines are appropriately followed, ICANN will:

- Require each evaluation panelist (provider and individual) to acknowledge and document understanding of the Conflict of Interest guidelines.
- Require each evaluation panelist to disclose all business relationships engaged in at any time during the past six months.
- Where possible, identify and secure primary and backup providers for evaluation panels.
- In conjunction with the evaluation panelists, develop and implement a process to identify conflicts and re-assign applications as appropriate to secondary or contingent third-party providers to perform the reviews.

Compliance Period -- All evaluation panelists must comply with the Conflict of Interest guidelines beginning with the opening date of the application submission period and ending with the public announcement by ICANN of the final outcomes of all the applications from the applicant in question.

Guidelines -- The following guidelines are the minimum standards with which all evaluation panelists must comply. It is recognized that it is impossible to foresee and cover all circumstances in which a potential conflict of interest might arise. In these cases, the evaluation panelist should evaluate whether the existing facts and circumstances would lead a reasonable person to conclude that there is an actual conflict of interest.

Evaluation Panelists and Immediate Family Members:

- Must not be under contract, have, or be included in a current proposal to provide professional services for or on behalf of the applicant during the compliance period.
- Must not currently hold or be committed to acquire any interest in a privately-held applicant organization.

- Must not currently hold or be committed to acquire more than 1% of any publicly listed applicant's outstanding equity securities or other ownership interests.
- Must not be involved or have an interest in a joint venture, partnership, or other business arrangement with the applicant.
- Must not have been named in a lawsuit with or against the applicant.
- Must not be a:
    - Director, officer, or employee, or in any capacity equivalent to that of a member of management of the applicant;
    - Promoter, underwriter, or voting trustee of the applicant; or
    - Trustee for any pension or profit- sharing trust of the applicant.

Definitions –

Evaluation panelist: An evaluation panelist is any individual associated with the review of an application. This includes primary, secondary, and contingent third-party panelists engaged by ICANN to review RSP applications.

Immediate family member: Immediate family member is a spouse, spousal equivalent, or dependent (whether or not related) of an evaluation panelist.

Professional services: These include, but are not limited to, legal services, financial audit, financial planning/investment, outsourced services, consulting services such as business/ management/internal audit, tax, information technology, registry/registrar services.

6.3.2. Conflict of Interest Violations

Breaches of the Conflict of Interest guidelines by evaluation panelists, whether intentional or not, shall be reviewed by ICANN org, which may make recommendations for corrective action, if deemed necessary. Serious breaches of the Conflict of Interest guidelines may be cause for dismissal of the person, persons, or provider committing the infraction.

In a case where ICANN org determines that a panelist has failed to comply with the Conflict of Interest guidelines, the results of that panelist's review for all assigned applications will be discarded and the affected applications will undergo a review by new panelists.

Complaints about violations of the Conflict of Interest by a panelist may be brought to the attention of ICANN org via the Public Comment and applicant support mechanisms throughout the evaluation period. Concerns of applicants regarding panels should be communicated via the defined support channels. Concerns of the general public (i.e., non-applicants) can be raised via the Public Comment forum.

6.4. Communications Channels

Defined channels for technical support or exchanges of information with ICANN org and with evaluation panels are available to applicants during the RSP evaluation periods via the RSP Portal. Contacting individual ICANN staff members, Board members, or individuals engaged by ICANN to perform an evaluation role in order to lobby for a particular outcome or to obtain confidential information about applications under review is not appropriate. In the interests of fairness and equivalent treatment for all applicants, any such individual contacts will be referred to the use of the RSP Portal.

7. Registry System Testing (RST)

Every RSP applicant is required to undergo Registry System Testing (RSTs) for the types of RSP for which they are applying.

These plans make use of existing test suites used for “business as usual” tests (such as pre-delegation tests, RSP transition tests, and changes to Registry Services), as well as new test suites designed specifically for the RSP evaluation program.

7.1. Evaluation Methodology

RST will follow the same methodology as that used for conducting “business as usual” RSTs. In summary, the process is as follows:

1. The RSP portal will create test request objects for each type of RSP being applied for and, in the case of IDNs, a test object per IDN Table being evaluated. Certain test parameters will be pre-defined at the time of creation and are determined by the information provided by the applicant.
2. The applicant must then configure its system to accommodate the test. This will involve creating test TLD(s) and registrar account(s), scheduling certain operational processes, and adding IP address information to its firewalls to allow ICANN org to access its registry services. Any information or resources needed to carry out this step will be provided in the RST system.
3. The applicant must then submit the required input parameters via the RST-API. These parameters include but are not limited to service hostnames, authentication credentials, service parameters, and samples of various file formats.
4. The applicant then uses the RST-API to initiate the test. Testing is fully automated. Applicants can use the API to monitor the progress and outcome of the test.
5. If the test passes, the process is completed and the application can proceed into the next phase.

6. If the test fails, or an error occurs, then the applicant can use the API to reset the test, reconfigure its systems, resubmit input parameters, and start a new test run. This may be repeated as often as necessary until a pass result is achieved.
7. Applicants may seek help regarding these tests using the RSP Portal.

7.2. Main RSP Registry System Testing

The Main RSP test plan is a subset of the standard pre-delegation and RSP transition test, and covers the following areas:

- **Extensible Provisioning Protocol (EPP):** This test suite validates the applicant's implementation of the Extensible Provisioning Protocol. The EPP service will be tested to ensure conformance with the RFC specifications and the requirements of the Registry Agreement.
- **Registration Data Access Protocol (RDAP):** This test suite validates the applicant's implementation of the RDAP service. This test suite is based on ICANN's existing RDAP Conformance Tool (rdapct)[2]. The test verifies compliance with the relevant RFCs, the ICANN RDAP Technical Implementation Guide[3], and the ICANN RDAP Response Profile [4].
- **Registry Data Escrow (RDE):** This test verifies that the applicant can generate a data escrow deposit that complies with the relevant RFCs, the requirements of the Registry Agreement, and ICANN's reporting requirements.
- **Internationalized Domain Names (IDN):** This test verifies the applicant's ability to comply with the relevant RFCs and guidelines for the IDN tables offered, including its ability to support provision of IDN variants as described in 4.1.12. Internationalized Domain Name (IDN) Evaluation.
- **Minimum Rights Protection Mechanisms (RPMs):** This test verifies the applicant's ability to comply with the minimum RPMs defined in the Registry Agreement, specifically, support for sunrise periods and trademark claims, and the Extensible Provisioning Protocol (EPP) launch extension (RFC 8334).

7.3. DNSSEC RSP Registry System Testing

For RSPs wishing to offer DNSSEC signing services, the DNSSEC RSP test plan includes the DNSSEC test suite used during pre-delegation and RSP transition tests, by including an additional suite focussed on DNSSEC operations.

In the DNSSEC operations suite, applicants must demonstrate that they are able to carry out

[2] https://github.com/icann/rdap-conformance-tool
[3] https://www.icann.org/en/system/files/files/rdap-technical-implementation-guide-15feb19-en.pdf
[4] https://www.icann.org/en/system/files/files/rdap-response-profile-15feb19-en.pdf

the operational practices outlined in RFC 6781, namely KSK/ZSK/CSK and algorithm rollovers for large zones.

7.4. DNS RSP Registry System Testing

For RSPs wishing to offer Authoritative DNS services, the DNS RSP test plan is based on the Authoritative DNS test suite used for pre-delegation and RSP transition tests. It verifies the service's conformance to the RFCs and the relevant specifications of the Registry Agreement.

7.5. Proxy RSP Registry System Testing

For RSPs wishing to offer an SRS Gateway service to provide compliance in a designated jurisdiction, the proxy RSP test suite is based on the SRS Gateway test suite used when an RO submits a request to add this registry service to their TLD(s). It tests the integration between the proxy RSP's infrastructure (EPP and RDAP services) and the primary RSP's services, specifically EPP, RDAP, and DNS services.

7.6. Testing Setup

To initiate RST, applicants will provide credentials and other information necessary for the RST service to access the applicant's registry systems. This information is provided via the RSP Portal.

Test plans within RST are provisioned according to the type of applications under consideration (e.g., Main RSP, DNS RSP, etc.). Each test plan is composed of multiple test suites, where each test suite is a set of inter-dependent test cases.

Formal definitions of the RST test plans, test suites, and tests cases may be found in GitHub.

7.7. Testing Process

Usage of the RST service is self-paced and under the control of each applicant. The RST service is commanded via an API. Applicants invoke each test case using this API, and may repeat tests as often as is necessary.

The definition of the RST-API may be found here.

8. RSP Evaluation Program – Terms and Conditions

The Terms and Conditions of the RSP Evaluation Program are available at [TBD_URL].

Appendix A. RSP Application Technical Questions

The questions provided in this document will appear in the RSP Portal, the on-line system to be used for RSP Evaluation applications, in the manner noted for each question and in the order and sections given in this document.

The following questions are broken into multiple sections. Many of the questions are common to each type of RSP. When questions are common to each type of RSP, this is noted.

Depending on the questions, answers are to be provided in various ways. When answers are free text, a character limit will be specified. Some answers will require attachments of diagrams. Some questions will require an answer of Yes or No, where an answer of No may indicate a failing score. In the RSP Portal, these questions will allow applicants to provide explanatory comments when the applicant selects No. These comments will be passed on to the evaluator for a final determination of a pass/fail score.

Some questions pertain to types of anycast DNS in which a distinction between global and non-global is necessary. Global anycast DNS refers to DNS service intended to serve DNS queries to any client throughout the world (e.g., over transit links). Non-global anycast DNS refers to DNS service intended to serve DNS queries to specific parts of the world (e.g., over peering at an IxP).

Main RSP

The Main RSP is responsible for the creation and maintenance of domain name registrations in a Shared Registration System (SRS). This encompasses the lifecycle of domain name registrations using protocols such as the Extensible Provisioning Protocol (EPP), and adherence to policies regarding transparency of domain name registrations through reporting, the Registration Data Access Protocol (RDAP), data escrow of domain registration data, and other functions.

Applications to be a Main RSP are not evaluated in relation to Authoritative DNS and DNSSEC services. Organizations should separately apply to be a DNS and/or DNSSEC RSP if those services are offered to Registry Operators.

MAIN.1. Security Controls

Provide a summary of the security controls for the proposed registry service provider, encompassing both physical security and logical security regarding the operation of gTLD

registry services. This information applies to in-house and all third-party (e.g. cloud providers, software vendors) vendors relevant to the registry services under application.

Provide answers for the following:

MAIN.1.1. Third-Party Certificate

Does or will this RSP have a publicly verifiable, 3rd party certification (e.g. ISO 27001) held directly by the organization and relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.2. Information Security Management System

Describe the information security management system (ISMS) implemented by this RSP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.1.3. Physical Access Controls

Does or will this RSP have processes and controls to manage physical access to infrastructure and systems, including building access controls, security cameras and/or other sensors, physical environmental monitoring and safety equipment, and alarm systems related to the physical infrastructure?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.4. System Access Controls

Does or will this RSP have processes and controls to manage non-physical access to infrastructure, including network access from both internal systems and external Internet systems, intrusion detection systems, security information and event management systems, network firewalls, network segmentation and isolation, user identification and authentication, and authorization schemes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.5. Vendor Management

Does or will this RSP have processes and controls pertaining to the selection of vendors

and equipment suppliers, management and maintenance of assets while in use, procurement of assets, and safe disposal of assets?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.6. Cryptographic Material

Does or will this RSP routinely renew and keep safe all cryptographic material necessary for the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.7. Secure Data At-Rest

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) at-rest data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.8. Secure Data In-Transit

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) in-transit data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.9. Virtualization Controls

If applicable, does or will this RSP have security controls for data in virtualized environments, including controls relevant to both on-premises or private virtualization environments as well as public clouds, network isolation, memory isolation, process isolation, and hypervisor access controls?

- Answer format: Yes, No, or Not Applicable.
- This is a sub-question common to all types of RSP.

MAIN.1.10. CISO

Does or will this RSP have a senior executive primarily in charge of and responsible for security?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.11. Emerging Threats

Describe the dedicated resources used to address emerging threats. This includes, but is not limited to, the utilization of either an in-house or third-party Computer Emergency Response Team (CERT), penetration testing schedule, software supply chain scanning, and participation in DNS, network, and/or security related forums (e.g. NANOG, RIPE, DNS-OARC).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.1.12. Background Checks

Does or will this RSP conduct background checks, both initial and on-going, of personnel and vendors relevant to the registry services under application for criminal history, fiduciary conflicts of interest, fraudulent bona fides, and indicators of current or potential corruption?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.13. DDOS

Describe the solutions and mitigations to be used to thwart Distributed Denial of Service (DDOS) attacks.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.1.14. BCP 38

Does or will this RSP implement BCP 38?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.1.15. Secure Routing

Does or will this RSP implement routing security of some nature, such as automated route filters, RPKI route origin validation, or other operational practices defined by the Internet Society's Mutually Agreed Norms for Routing Security (MANRS)?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2. Technical Overview

Provide a technical overview of the systems, software, and technical practices of the registry service provider.

Provide answers for the following:

MAIN.2.1. Systems and Software

Describe the systems and software relating to the operation of the RSP and the purpose and function for each. This must include, but is not limited to, types of operating systems, application software, programming languages, virtualization environments, network elements, appliances, and sizing requirements. The given list must contain software and systems which are both modern and in common use.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This is a sub-question common to all types of RSP.

MAIN.2.2. Standard Hardware Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.3. Standard Software Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.4. Standard Hardware Lifecycle

Does or will this RSP have documented, regular, and active practices for the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.5. Secure Software Development

Does or will this RSP have documented, regular, and active practices for the secure development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.6. Hardware Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.7. Software Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.8. Hardware Lifecycle Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.9. Software Development Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.10. IaC

Does or will this RSP use Infrastructure-as-Code (IaC) to manage all systems relevant to operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.2.11. Automated Orchestration

Does or will this RSP use automated orchestration to manage all systems relevant to the operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.3. Architecture

Provide an architectural overview of the systems and software of the registry service provider, including descriptions of software architecture, systems dependencies, data flow within the registry, and logical systems interconnections.

Provide answers for the following:

MAIN.3.1. Network Architecture

Describe the network architecture relevant to the registry services under application. This includes, but is not limited to, descriptions of network segmentation, interior and exterior routing schemes, virtual private networks, and IP addressing plans.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

MAIN.3.2. Fault Tolerance

Describe the methods for resiliency of servers, including the use of load balancers, proxies, reverse proxies, caches, and other network elements.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

MAIN.3.3. Tier III Data Center

Does or will this RSP have at least two Tier III (as defined here: https://uptimeinstitute.com/tiers) or equivalent data centers having no inter-dependencies?

- Answer format: Yes or No.

- This answer must include an attachment of the certification or equivalent documentation in either JPG, PNG, or PDF format.
- Relevant Link: [Uptime Institute](https://uptimeinstitute.com/tiers)

MAIN.3.4. SRS to DNSSEC Data Transfer

Describe the data replication from the SRS to the DNS signing infrastructure, whether in-house or third-party (i.e. Main RSP -> DNSSEC RSP).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

MAIN.4. Data Store

Describe the data store used by the registry service provider, including performance characteristics, backup and recovery procedures, schema and schema evolution practices, security, and other relevant information.

Provide answers for the following:

MAIN.4.1. Data Storage

Describe how the technology used to store registration data ensures high availability and fault tolerance in order to meet the Service Level Requirements of the ICANN Registry Agreement.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.4.2. Data Replication

Describe how data is replicated between data centers in order to meet the Service Level Requirements of the ICANN Registry Agreement.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.4.3. On-site Backups

Does or will this RSP have on-site backups of registration data?

- Answer format: Yes or No.

MAIN.4.4. Off-site Backups

Does or will this RSP have off-site backups of registration data?

- Answer format: Yes or No.

MAIN.4.5. Data Retention

Does or will this RSP practice data retention policies with regard to backups of registration data?

- Answer format: Yes or No.

MAIN.4.6. Registration Data Backups

Does or will this RSP practice documented standards regarding media and data backups for registration data?

- Answer format: Yes or No.

MAIN.4.7. Recovery Practices

Does or will this RSP practice regularly scheduled validation of registration data backups, separately from recovery practices?

- Answer format: Yes or No.

MAIN.4.8. Scheduled Recovery

Does or will this RSP practice regularly scheduled recovery of registration data backups?

- Answer format: Yes or No.

MAIN.4.9. Production Data

Does or will this RSP forbid the use of production data in testing and/or development environments?

- Answer format: Yes or No.

MAIN.4.10. Schema Changes

Describe the practices regarding the changing of schemas and non-automated mutations to registration data in the data store for the purposes of mitigating the risk of downtime and outages.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.4.11. Data Throughput

Provide the peak and sustained throughput of transactional data written to and read from

the data store, maximum capacity in raw and materialized registration data in the data store, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.4.12. Encrypted Registration Data At-Rest

Does or will this RSP encrypt registration data at-rest in the data store?

- Answer format: Yes or No.

MAIN.4.13. Encrypted Registration Data In-Transit

Does or will this RSP encrypt registration data in-transit to and from the data store?

- Answer format: Yes or No.

MAIN.4.14. Cryptographic Material Renewal

Does or will this RSP regularly and frequently renew the cryptographic material used for the encryption of registration data both at-rest and in-transit with regard to the data store in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.4.15. Cryptographic Material Handling

Does or will this RSP keep safe the cryptographic material used for the encryption of registration data both at-rest and in-transit with regard to the data store in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.4.16. Cryptographic Algorithms

Does or will this RSP use modern and known-secure cryptographic algorithms for the encryption of registration data at-rest and in-transit with regard to the data store?

- Answer format: Yes or No.

MAIN.4.17. Customer Data

Describe the security controls of customer credentials, personal data, and sensitive information, including access and recovery of this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.4.18. Hashing Algorithms

Describe the hashing algorithms used for the storage of customer credentials, including all relevant parameters (e.g. work factor).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.5. EPP Service

Describe the use of the Extensible Provisioning Protocol (EPP) by the registry service provider. Provide details on usage of EPP extensions, performance characteristics, security controls to be used with EPP, and other technical details.

Provide answers for the following:

MAIN.5.1. RFC 5730

Does or will this RSP implement RFC 5730 (“Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes or No.

MAIN.5.2. RFC 5731

Does or will this RSP implement RFC 5731 (“Extensible Provisioning Protocol (EPP) Domain Name Mapping”)?

- Answer format: Yes or No.

MAIN.5.3. RFC 5734

Does or will this RSP implement RFC 5734 (“Extensible Provisioning Protocol (EPP) Transport over TCP”)?

- Answer format: Yes or No.

MAIN.5.4. RFC 5910

Does or will this RSP implement RFC 5910 (“Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes or No.

MAIN.5.5. RFC 5733

If applicable, does or will this RSP implement RFC 5733 (“Extensible Provisioning Protocol (EPP) Contact Mapping”)?

- Answer format: Yes, No, or Not Applicable.

MAIN.5.6. RFC 8334

If applicable, does or will this RSP implement RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes, No, or Not Applicable.

MAIN.5.7. RFC 8334 Mechanisms

If RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”) is not applicable to this RSP, describe the mechanism to support sunrise and claims in EPP. Please answer with “Not Applicable” or “N/A” if this RSP does or will implement RFC 8334.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- Note that this question does not need to be answered if the RSP does implement RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”). See sub-question above.

MAIN.5.8. EPP Contacts

Does or will this RSP forbid access to contacts via EPP to registrars other than the sponsoring registrar?

- Answer format: Yes or No.

MAIN.5.9. EPP Extensions

Provide a list of all EPP extensions to be used that are registered in the IANA EPP extensions registry, and an attestation that all EPP extensions to be used are registered with the IANA as per RFC 7451 (“Extension Registry for the Extensible Provisioning Protocol”).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.5.10. Unregistered EPP Extensions

Does or will this RSP forgo the use of any EPP extensions which are not registered with the IANA as per RFC 7451 (“Extension Registry for the Extensible Provisioning Protocol”)?

- Answer format: Yes or No.

MAIN.5.11. EPP Performance

Does or will this RSP implement and operate EPP according to the performance requirements defined in Specification 10 of the ICANN Registry Agreement?

- Answer format: Yes or No.

MAIN.5.12. EPP Equal Access

Does or will this RSP have controls to prevent EPP misuse and ensure all registrars have fair and equal access to EPP per Specification 9 of the ICANN Registry Agreement?

- Answer format: Yes or No.

MAIN.5.13. EPP Client Connections

Describe how data integrity is achieved across multiple client connections, including but not limited to usage of soft-state and eventual consistency if applicable, and the application of Atomicity, Consistency, Isolation, and Durability (ACID) principles.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.5.14. RFC 9325

Does or will this RSP implement RFC 9325 (“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”) notwithstanding RFC 5734 (“Extensible Provisioning Protocol (EPP) Transport over TCP”)? Note: while RFC 9325 covers TLS and DTLS, EPP only uses TLS.

- Answer format: Yes or No.

MAIN.5.15. EPP Cryptographic Material Renewal

Does or will this RSP regularly and frequently renew the cryptographic material used to secure EPP communications in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.5.16. EPP Cryptographic Material Handling

Does or will this RSP keep safe the cryptographic material used to secure EPP communication in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.5.17. EPP Reporting

Does or will this RSP comply with Specification 3 of the ICANN Registry Agreement with respect to EPP?

- Answer format: Yes or No.

MAIN.5.18. EPP Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the EPP service in such a manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to EPP (excluding system services such as monitoring, remote access and NTP)?

- Answer format: Yes or No.

MAIN.6. RDAP

Describe the use of the Registration Data Access Protocol (RDAP) by the registry service provider. Provide details on usage of RDAP extensions, performance characteristics, security controls to be used with RDAP, and other technical details.

Provide answers for the following:

MAIN.6.1. RFC 7480

Does or will this RSP implement RFC 7480 (“HTTP Usage in the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

MAIN.6.2. RFC 7481

Does or will this RSP implement RFC 7481 (“Security Services for the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

MAIN.6.3. Current RFC 8521

Does or will this RSP implement RFC 8521 (“Registration Data Access Protocol (RDAP) Object Tagging”) for all currently operated gTLDs?

- Answer format: Yes or No.

MAIN.6.4. Future RFC 8521

Does this RSP plan to continue to implement RFC 8521 (“Registration Data Access Protocol (RDAP) Object Tagging”) for all gTLDs operated in the future?

- Answer format: Yes or No.

MAIN.6.5. RFC 9082

Does or will this RSP implement RFC 9082 (“Registration Data Access Protocol (RDAP) Query Format”)?

- Answer format: Yes or No.

MAIN.6.6. RFC 9083

Does or will this RSP implement RFC 9083 (“JSON Responses for the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

MAIN.6.7. Current RFC 9224

Does or will this RSP implement RFC 9224 (“Finding the Authoritative Registration Data Access Protocol (RDAP) Service”) for all currently operated gTLDs?

- Answer format: Yes or No.

MAIN.6.8. Future RFC 9224

Will this RSP implement RFC 9224 (“Finding the Authoritative Registration Data Access Protocol (RDAP) Service”) for all gTLDs operated in the future?

- Answer format: Yes or No.

MAIN.6.9. RDAP Technical Implementation Guide

Does or will this RSP implement the ICANN gTLD RDAP Technical Implementation Guide?

- Answer format: Yes or No.

MAIN.6.10. RDAP Response Profile

Does or will this RSP implement the ICANN gTLD RDAP Response Profile?

- Answer format: Yes or No.

MAIN.6.11. RDAP Extensions

Provide a list of all RDAP extensions to be used.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.6.12. Unregistered RDAP Extensions

Does or will this RSP forgo the use of any RDAP extensions which are not registered

with the IANA as per RFC 7480 (“HTTP Usage in the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

MAIN.6.13. RDAP Performance

Does or will this RSP comply with the Service Level Agreements of the ICANN Registry Agreement (Specification 10) with regard to RDAP?

- Answer format: Yes or No.

MAIN.6.14. RDAP Data Mining

Does or will this RSP implement methods to prevent mining of registration data via RDAP?

- Answer format: Yes or No.

MAIN.6.15. RFC 9325

Does or will this RSP implement RFC 9325 (“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”) with respect to RDAP? Note: while RFC 9325 covers TLS and DTLS, RDAP only uses TLS.

- Answer format: Yes or No.

MAIN.6.16. RDAP Cryptographic Material Renewal

Does or will this RSP regularly and frequently renew the cryptographic material used to secure RDAP communications in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.6.17. RDAP Cryptographic Material Handling

Does or will this RSP keep safe the cryptographic material used to secure RDAP communication in accordance with industry best common practices?

- Answer format: Yes or No.

MAIN.6.18. RDAP Reporting

Does or will this RSP comply with Specification 3 of the ICANN Registry Agreement with respect to RDAP?

- Answer format: Yes or No.

MAIN.6.19. RDAP Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the RDAP service in such a

manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to RDAP (excluding system services such as monitoring, remote access and NTP)?

- Answer format: Yes or No.

MAIN.7. Internet Connectivity

Describe the IPv4 and IPv6 connectivity and reachability of the registry service provider, including performance characteristics, transit, cloud, and/or backbone providers, peering exchanges, routing stability and other information.

Provide answers for the following:

MAIN.7.1. IPv4 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv4 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.7.2. IPv6 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv6 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.7.3. IPv4 RDAP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to RDAP and IPv4?

- Answer format: Yes or No.

MAIN.7.4. IPv4 EPP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to EPP and IPv4?

- Answer format: Yes or No.

MAIN.7.5. IPv6 RDAP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to RDAP and IPv6?

- Answer format: Yes or No.

MAIN.7.6. IPv6 EPP

Will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to EPP and IPv6 if requested by a registrar?

- Answer format: Yes or No.

MAIN.8. Abuse Prevention and Mitigation

Describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users.

Provide answers for the following:

MAIN.8.1. Domain Registration Abuse

Will this RSP provide tools and mechanisms to Registry Operators for the purposes of automated processing and identification of abusive domain registrations.

- Answer format: Yes or No.

MAIN.8.2. EPP and RDAP Status Values

Describe the EPP and RDAP status values as they relate to domain name registrations considered to be abusive registrations and those not considered to be abusive registrations.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.9. Rights Protection

Describe the tools that may be used by a gTLD to comply with the policies and practices of Rights Protection Management.

Provide answers for the following:

MAIN.9.1. URS

Describe the EPP and RDAP status values and their applicability to Uniform Rapid Suspension (URS).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.9.2. RFC 9361

Does or will this RSP implement the Registry Operator-related elements of RFC9361

- Answer format: Yes or No.

MAIN.10. Registration Lifecycle

Provide a detailed description of the proposed registration lifecycle for domain names. Explain the various registration states, state transition timelines, and relationship of these states with EPP and RDAP.

Provide answers for the following:

MAIN.10.1. Registration Lifecycle

Describe all potential registration lifecycle(s) of domain names supported in the system.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

MAIN.10.2. Domain Registration Values

Describe the registration lifecycle(s) of domain names with respect to EPP status values and RDAP status values.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.10.3. Nameserver Registration Values

Describe the nameserver host lifecycle, including relevance to EPP and RDAP status values, with respect to the lifecycle of domain names. This should include a description of nameservers as either attributes of domains or as host objects.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.10.4. Contact Registration Values

If applicable, describe the contact lifecycle, including relevance to EPP and RDAP status

values, with respect to the lifecycle of domain names and nameservers. Include a description of the deletion of orphaned contacts.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.10.5. Orphaned Glue

Does or will this RSP be capable of removing orphaned glue in accordance with Specification 6 of the ICANN Registry Agreement?

- Answer format: Yes, No or Not Applicable.

MAIN.10.6. BRDA

Describe the systems, software, and processes used to integrate to ICANN's Bulk Registration Data Access (BRDA, Specification 4 of the Registry Agreement), ICANN's Registration Reporting System (RRI, Specification 2 and Specification 3 of the Registry Agreement), and ICANN's Zone File Access (ZFA, Specification 4 of the Registry Agreement).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.10.7. Data Escrow

Describe how this RSP will comply with Specification 2 of the Registry Agreement, and describe any other data escrow processes. This includes escrow extensions for data related additional registry services.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

MAIN.11. Registry Continuity

Describe how the registry service provider will comply with registry continuity, including but not limited to obligations as described in Specification 6 (section 3) to the Registry Agreement. This includes conducting registry operations using diverse, redundant servers to ensure continued operation of critical functions in the case of technical failure.

Provide answers for the following:

MAIN.11.1. Registry Continuity Exercise

Does or will this RSP regularly exercise registry continuity actions?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.11.2. Registry Continuity Compliance

Describe how this RSP will be in compliance with Specification 6.3 of the ICANN Registry Agreement.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.11.3. EBERO

Does or will this RSP participate in coordinated Emergency Back-end Registry Operator (EBERO) transitions, including but not limited to maintaining the DNSSEC chain of trust, of hosted gTLDs when the business relationship of this RSP and the Registry Operator is not in good standing?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12. Monitoring and Fault Escalation

Describe arrangements for monitoring critical registry systems (including SRS, database systems, EPP services, RDAP services, network connectivity, routers and firewalls). This description should explain how these systems are monitored and the mechanisms that will be used for fault escalation and reporting, and should provide details of the proposed support arrangements for these registry systems.

Provide answers for the following:

MAIN.12.1. Internal Monitoring

Does or will this RSP monitor for faults inside its own network?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12.2. External Monitoring

Does or will this RSP monitor for faults from a point outside any of its own networks?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12.3. Fault Triage

Does or will this RSP have documented processes for aggregation and triage of faults?

- Answer format: Yes or No.

- This is a sub-question common to all types of RSP.

MAIN.12.4. Fault Mitigation

Does or will this RSP have documented processes to mitigate faults once detected?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12.5. Regional Points of Presence

Provide a list of at least one point of presence where fault monitoring is conducted from each of the continents of North America, Central or South America, Asia, Europe, and Africa.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.12.6. Fault Minimization

Does or will this RSP have processes to minimize faults during maintenance of systems, including both automated processes and manual change control processes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12.7. On-call Staff

Does or will this RSP have personnel capable of reacting to and mitigating faults 24 hours per day of every day of every year of service?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

MAIN.12.8. Service Disruptions

Provide documentation regarding any RSP functions currently being served for any gTLD, the domain names of the gTLDs, and all service disruptions for each gTLD in the past six months, where a service disruption is defined by Specification 10 of the Registry Agreement).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.13. Capacity

Provide a summary of capacity capabilities and other information necessary for the adequate approval of the RSP to accommodate the projected forecast of gTLD(s). The Main RSP should

at least support the aggregate of the expected number of domain names within 3 years for all TLDs using the RSP plus the currently supported TLDs, if any.

Provide answers for the following:

MAIN.13.1. DUMs per TLD

Provide the maximum number of Domains Under Management (DUMs) per TLD, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.13.2. Maximum TLDs

Provide the maximum number of TLDs that may be serviced, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.13.3. Current DUMs

Provide the current TLDs being serviced and the DUMs for each, if any.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.13.4. Maximum Capacity

Provide the maximum number of TLDs and combined DUMs that can be serviced from the least-capable data center. If service is provided using public cloud services, provide the maximum capacity based on the contracted resources. Describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

MAIN.13.5. Available Load

Provide documentation that either services contracted from a public cloud provider or services provided from private sources demonstrate the needed capacity as stated

above. This documentation may include, but is not limited to, number of servers, contracted bandwidth from network providers, and load test reports.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS RSP

The DNS RSP is responsible for providing DNS infrastructure and service for a TLD. A DNS RSP does not pertain to providing the Shared Registration System (SRS) components or DNSSEC components necessary for a TLD. Organizations should apply to be a Main RSP and/or DNSSEC RSP separately if providing those services is being sought.

A DNS RSP must implement anycast to all DNS nameservers, and must document anycast DNS nodes that provide limited, localized, or non-global anycast service.

DNS.1. Security Controls

Provide a summary of the security controls for the proposed registry service provider, encompassing both physical security and logical security regarding the operation of gTLD registry services. This information applies to in-house and all third-party (e.g. cloud providers, software vendors) vendors relevant to the registry services under application.

Provide answers for the following:

DNS.1.1. Third-Party Certificate

Does or will this RSP have a publicly verifiable, 3rd party certification (e.g. ISO 27001) held directly by the organization and relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.2. Information Security Management System

Describe the information security management system (ISMS) implemented by this RSP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.1.3. Physical Access Controls

Does or will this RSP have processes and controls to manage physical access to

infrastructure and systems, including building access controls, security cameras and/or other sensors, physical environmental monitoring and safety equipment, and alarm systems related to the physical infrastructure?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.4. System Access Controls

Does or will this RSP have processes and controls to manage non-physical access to infrastructure, including network access from both internal systems and external Internet systems, intrusion detection systems, security information and event management systems, network firewalls, network segmentation and isolation, user identification and authentication, and authorization schemes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.5. Vendor Management

Does or will this RSP have processes and controls pertaining to the selection of vendors and equipment suppliers, management and maintenance of assets while in use, procurement of assets, and safe disposal of assets?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.6. Cryptographic Material

Does or will this RSP routinely renew and keep safe all cryptographic material necessary for the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.7. Secure Data At-Rest

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) at-rest data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.8. Secure Data In-Transit

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) in-transit data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.

- This is a sub-question common to all types of RSP.

DNS.1.9. Virtualization Controls

If applicable, does or will this RSP have security controls for data in virtualized environments, including controls relevant to both on-premises or private virtualization environments as well as public clouds, network isolation, memory isolation, process isolation, and hypervisor access controls?

- Answer format: Yes, No, or Not Applicable.
- This is a sub-question common to all types of RSP.

DNS.1.10. CISO

Does or will this RSP have a senior executive primarily in charge of and responsible for security?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.11. Emerging Threats

Describe the dedicated resources used to address emerging threats. This includes, but is not limited to, the utilization of either an in-house or third-party Computer Emergency Response Team (CERT), penetration testing schedule, software supply chain scanning, and participation in DNS, network, and/or security related forums (e.g. NANOG, RIPE, DNS-OARC).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.1.12. Background Checks

Does or will this RSP conduct background checks, both initial and on-going, of personnel and vendors relevant to the registry services under application for criminal history, fiduciary conflicts of interest, fraudulent bona fides, and indicators of current or potential corruption?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.13. DDOS

Describe the solutions and mitigations to be used to thwart Distributed Denial of Service (DDOS) attacks.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

- This is a sub-question common to all types of RSP.

DNS.1.14. BCP 38

Does or will this RSP comply with BCP 38?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.1.15. Secure Routing

Does or will this RSP implement routing security of some nature, such as automated route filters, RPKI route origin validation, or other operational practices defined by the Internet Society's Mutually Agreed Norms for Routing Security (MANRS)?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2. Technical Overview

Provide a technical overview of the systems, software, and technical practices of the registry service provider.

Provide answers for the following:

DNS.2.1. Systems and Software

Describe the systems and software relating to the operation of the RSP and the purpose and function for each. This must include, but is not limited to, types of operating systems, application software, programming languages, virtualization environments, network elements, appliances, and sizing requirements. The given list must contain software and systems which are both modern and in common use.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This is a sub-question common to all types of RSP.

DNS.2.2. Standard Hardware Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.3. Standard Software Maintenance

Does or will this RSP have documented, regular, and active practices for the

maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.4. Standard Hardware Lifecycle

Does or will this RSP have documented, regular, and active practices for the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.5. Secure Software Development

Does or will this RSP have documented, regular, and active practices for the secure development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.6. Hardware Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.7. Software Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.8. Hardware Lifecycle Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.9. Software Development Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.10. IaC

Does or will this RSP use Infrastructure-as-Code (IaC) to manage all systems relevant to operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.2.11. Automated Orchestration

Does or will this RSP use automated orchestration to manage all systems relevant to the operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.3. Architecture

Provide an architectural overview of the systems and software of the registry service provider, including descriptions of software architecture, systems dependencies, data flow within the registry, and logical systems interconnections.

Provide answers for the following:

DNS.3.1. Network Architecture

Describe the network architecture relevant to the registry services under application. This includes, but is not limited to, descriptions of network segmentation, interior and exterior routing schemes, virtual private networks, and IP addressing plans.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

DNS.3.2. Fault Tolerance

Describe the methods for resiliency of servers, including the use of load balancers, proxies, reverse proxies, caches, and other network elements.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

DNS.3.3. DNS Resiliency

Describe the methods resiliency for DNS, including the use of anycast, primary and secondary DNS authoritative servers, and hidden DNS zone transfer servers.

- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNS.3.4. DNS Zone Distribution Data Center

Does or will this RSP have at least two Tier III (as defined here: https://uptimeinstitute.com/tiers) or equivalent data centers having no inter-dependencies for DNS zone distribution?

- Answer format: Yes or No.
- This answer must include an attachment of the certification or equivalent documentation in either JPG, PNG, or PDF format.
- Relevant Link: [Uptime Institute](https://uptimeinstitute.com/tiers)

DNS.3.5. Anycast Data Center

Does or will this RSP have at least two Tier III or equivalent data centers having no inter-dependencies for global DNS anycast service?

- Answer format: Yes or No.
- This answer must include an attachment of the certification or equivalent documentation in either JPG, PNG, or PDF format.

DNS.3.6. DNSSEC to DNS Data Transfer

Description of data replication between DNS servers and data replication from the DNSSEC signing infrastructure to the DNS servers, whether in-house or with third-parties (i.e. DNSSEC RSP -> DNS RSP).

- The answer to this question will not be published.

- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNS.4. Geographic Diversity

Provide a description of the geographical diversity of services for the registry service provider. Describe the physical location of data centers and cloud providers, nameserver, back-up storage sites, and network operations centers.

Provide answers for the following:

DNS.4.1. Geographic DNS Service

Describe the geographic diversity for all DNS nodes, including detailed distinctions between unicast nodes, anycast nodes serving global traffic, and anycast nodes serving non-global, regional, or local traffic.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNS.4.2. Geographic Risk Mitigation

Provide evidence of a geographic, topological, and national diversity that greatly reduces the risk profile of the proposed registry by ensuring the continuance of the DNS Registry Service.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of separate documentation in either PNG, JPG, or PDF format.

DNS.4.3. DNS Failure

Does or will this RSP have enough coverage of DNS service to accommodate failures of any DNS point-of-presence to maintain minimum Service Level Requirements?

- Answer format: Yes or No.

DNS.5. DNS Service

Describe the nature, architecture, and operation of nameservers and DNS service, including compliance with the relevant DNS standards.

The response should include but is not limited to:

DNS.5.1. Service Architecture

Descriptions of service architecture for all DNS node types, including unicast nodes, anycast nodes serving global traffic, and anycast nodes serving non-global, regional, or local traffic.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNS.5.2. RFC 1034

Does or will this RSP implement RFC 1034 (“DOMAIN NAMES - CONCEPTS AND FACILITIES”)?

- Answer format: Yes or No.

DNS.5.3. RFC 1035

Does or will this RSP implement RFC 1035 (“DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION”)?

- Answer format: Yes or No.

DNS.5.4. RFC 1123

Does or will this RSP implement RFC 1123 (“Requirements for Internet Hosts -- Application and Support”)?

- Answer format: Yes or No.

DNS.5.5. RFC 1982

Does or will this RSP implement RFC 1982 (“Serial Number Arithmetic”)?

- Answer format: Yes or No.

DNS.5.6. RFC 2181

Does or will this RSP implement RFC 2181 (“Clarifications to the DNS Specification”)?

- Answer format: Yes or No.

DNS.5.7. RFC 3226

Does or will this RSP implement RFC 3226 (“DNSSEC and IPv6 A6 aware server/resolver message size requirements”)?

- Answer format: Yes or No.

DNS.5.8. RFC 3596

Does or will this RSP implement RFC 3596 (“DNS Extensions to Support IP Version 6”)?

- Answer format: Yes or No.

DNS.5.9. RFC 3597

Does or will this RSP implement RFC 3597 (“Handling of Unknown DNS Resource Record (RR) Types”)?

- Answer format: Yes or No.

DNS.5.10. RFC 4343

Does or will this RSP implement RFC 4343 (“Domain Name System (DNS) Case Insensitivity Clarification”)?

- Answer format: Yes or No.

DNS.5.11. RFC 6891

Does or will this RSP implement RFC 6891 (“Extension Mechanisms for DNS (EDNS(0)))”?

- Answer format: Yes or No.

DNS.5.12. RFC 7766

Does or will this RSP implement RFC 7766 (“DNS Transport over TCP - Implementation Requirements”)?

- Answer format: Yes or No.

DNS.5.13. RFC 5001

Does or will this RSP implement RFC 5001 (“DNS Name Server Identifier (NSID) Option”)?

- Answer format: Yes or No.

DNS.5.14. RFC 6186

Does or will this RSP operate DNS service according to RFC 6186 (“Use of SRV Records for Locating Email Submission/Access Services”)?

- Answer format: Yes or No.

DNS.5.15. RFC 8906

Does or will this RSP operate DNS service according to RFC 8906 (“A Common Operational Problem in DNS Servers: Failure to Communicate”)?

- Answer format: Yes or No.

DNS.5.16. RFC 9199

Does or will this RSP operate DNS service according to RFC 9199 (“Considerations for Large Authoritative DNS Server Operators”)?

- Answer format: Yes or No.

DNS.5.17. RFC 9210

Does or will this RSP operate DNS service according to RFC 9210 (“DNS Transport over TCP - Operational Requirements”)?

- Answer format: Yes or No.

DNS.5.18. DNS Performance

Does or will this RSP comply with the Service Level Agreements of the ICANN Registry Agreement (Specification 10) with regard to DNS?

- Answer format: Yes or No.

DNS.5.19. DNS Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the DNS service in such a manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to DNS (excluding system services such as monitoring, remote access and NTP)?

- Answer format: Yes or No.

DNS.5.20. DNS Software

Provide a list of DNS software implementations including version numbers, either open source, commercial, or proprietary.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

DNS.5.21. Individual Node Monitoring

Does or will this RSP monitor all unique DNS servers of all anycast nodes?

- Answer format: Yes or No.

DNS.5.22. IANA Compliance

Does or will this RSP operate authoritative DNS servers according to the IANA Technical Requirements for Authoritative Name Servers (https://www.iana.org/help/nameserver-requirements)?

- Answer format: Yes or No.

DNS.6. Internet Connectivity

Describe the IPv4 and IPv6 connectivity and reachability of the registry service provider, including performance characteristics, transit, cloud, and/or backbone providers, peering exchanges, routing stability and other information.

Provide answers for the following:

DNS.6.1. IPv4 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv4 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.6.2. IPv6 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv6 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.6.3. IPv4 Performance

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to DNS and IPv4?

- Answer format: Yes or No.

DNS.6.4. IPv6 Performance

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to DNS and IPv6?

- Answer format: Yes or No.

DNS.6.5. IPv4 Points of Presense

Provide a list of points of presence where IPv4 services are to be provided, including the number of IPv4 unicast, IPv4 global anycast and IPv4 non-global anycast DNS nodes at each point of presence.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer may include diagrams in either PNG, JPG, or PDF format.

DNS.6.6. IPv6 Points of Presense

Provide a list of points of presence where IPv6 services are to be provided, including the number of IPv6 unicast, IPv6 global anycast and IPv6 non-global anycast DNS nodes at each point of presence.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer may include diagrams in either PNG, JPG, or PDF format.

DNS.7. Registry Continuity

Describe how the registry service provider will comply with registry continuity, including but not limited to obligations as described in Specification 6 (section 3) to the Registry Agreement. This includes conducting registry operations using diverse, redundant servers to ensure continued operation of critical functions in the case of technical failure.

Provide answers for the following:

DNS.7.1. Registry Continuity Exercise

Does or will this RSP regularly exercise registry continuity actions?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.7.2. Registry Continuity Compliance

Describe how this RSP will be in compliance with Specification 6.3 of the ICANN Registry Agreement.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.7.3. EBERO

Does or will this RSP participate in coordinated Emergency Back-end Registry Operator (EBERO) transitions, including but not limited to maintaining the DNSSEC chain of trust, of hosted gTLDs when the business relationship of this RSP and the Registry Operator is not in good standing?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8. Monitoring and Fault Escalation Processes

Describe arrangements for monitoring critical registry systems (including DNS services, network connectivity, routers and firewalls). This description should explain how these systems are monitored and the mechanisms that will be used for fault escalation and reporting, and should provide details of the proposed support arrangements for these registry systems.

Provide answers for the following:

DNS.8.1. Internal Monitoring

Does or will this RSP monitor for faults inside its own network?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.2. External Monitoring

Does or will this RSP monitor for faults from a point outside any of its own networks?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.3. Fault Triage

Does or will this RSP have documented processes for aggregation and triage of faults?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.4. Fault Mitigation

Does or will this RSP have documented processes to mitigate faults once detected?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.5. Regional Points of Presense

Provide a list of at least one point of presence where fault monitoring is conducted from each of the continents of North America, Central or South America, Asia, Europe, and Africa.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.8.6. Fault Minimization

Does or will this RSP have processes to minimize faults during maintenance of systems, including both automated processes and manual change control processes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.7. On-call Staff

Does or will this RSP have personnel capable of reacting to and mitigating faults 24 hours per day of every day of every year of service?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNS.8.8. Service Disruptions

Provide documentation regarding any RSP functions currently being served for any gTLD, the domain names of the gTLDs, and all service disruptions for each gTLD in the past six months, where a service disruption is defined by Specification 10 of the Registry Agreement).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.8.9. Zone Pipelines

Describe the processes to insure accurate, complete and compliant DNS zones such as staged roll-outs, zone pipelines, and other quality assurance methodologies.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

DNS.8.10. Zone Consistency

Describe the processes to ensure the contents of the DNS zone from each DNS point-of-presence are consistent.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

DNS.9. Capacity

Provide a summary of capacity capabilities and other information necessary for the adequate approval of the RSP to accommodate the projected forecast of gTLD(s). The Main RSP should at least support the aggregate of the expected number of domain names within 3 years for all TLDs using the RSP plus the currently supported TLDs, if any.

Provide answers for the following:

DNS.9.1. DUMs per TLD

Provide the maximum number of Domains Under Management (DUMs) per TLD, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.9.2. Maximum TLDs

Provide the maximum number of TLDs that may be serviced, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.9.3. Current DUMs

Provide the current TLDs being serviced and the DUMs for each, if any.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.9.4. Maximum Capacity

Provide the maximum number of TLDs and combined DUMs that can be serviced from the least-capable data center. If service is provided using public cloud services, provide the maximum capacity based on the contracted resources. Describe the methods used to determine this information.

- The answer to this question will not be published.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNS.9.5. Available Load

Provide documentation that either services contracted from a public cloud provider or services provided from private sources demonstrate the needed capacity as stated above. This documentation may include, but is not limited to, number of servers, contracted bandwidth from network providers, and load test reports.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC RSP

The DNSSEC RSP is responsible for providing cryptographic operations relevant for the creation and safekeeping of DNSSEC key material and providing the necessary operations for the cryptographic signing of DNS zone data. Organizations should apply to be a Main RSP and/or DNS RSP separately if providing those services is being sought.

DNSSEC.1. Security Controls

Provide a summary of the security controls for the proposed registry service provider, encompassing both physical security and logical security regarding the operation of gTLD registry services. This information applies to in-house and all third-party (e.g. cloud providers, software vendors) vendors relevant to the registry services under application.

Provide answers for the following:

DNSSEC.1.1. Third-Party Certificate

Does or will this RSP have a publicly verifiable, 3rd party certification (e.g. ISO 27001) held directly by the organization and relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.2. Information Security Management System

Describe the information security management system (ISMS) implemented by this RSP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.1.3. Physical Access Controls

Does or will this RSP have processes and controls to manage physical access to infrastructure and systems, including building access controls, security cameras and/or other sensors, physical environmental monitoring and safety equipment, and alarm systems related to the physical infrastructure?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.4. System Access Controls

Does or will this RSP have processes and controls to manage non-physical access to infrastructure, including network access from both internal systems and external Internet systems, intrusion detection systems, security information and event management systems, network firewalls, network segmentation and isolation, user identification and authentication, and authorization schemes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.5. Vendor Management

Does or will this RSP have processes and controls pertaining to the selection of vendors and equipment suppliers, management and maintenance of assets while in use, procurement of assets, and safe disposal of assets?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.6. Cryptographic Material

Does or will this RSP routinely renew and keep safe all cryptographic material necessary for the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.7. Secure Data At-Rest

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) at-rest data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.8. Secure Data In-Transit

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) in-transit data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.9. Virtualization Controls

If applicable, does or will this RSP have security controls for data in virtualized environments, including controls relevant to both on-premises or private virtualization environments as well as public clouds, network isolation, memory isolation, process isolation, and hypervisor access controls?

- Answer format: Yes, No, or Not Applicable.
- This is a sub-question common to all types of RSP.

DNSSEC.1.10. CISO

Does or will this RSP have a senior executive primarily in charge of and responsible for security?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.11. Emerging Threats

Describe the dedicated resources used to address emerging threats. This includes, but is not limited to, the utilization of either an in-house or third-party Computer Emergency Response Team (CERT), penetration testing schedule, software supply chain scanning, and participation in DNS, network, and/or security related forums (e.g. NANOG, RIPE, DNS-OARC).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.1.12. Background Checks

Does or will this RSP conduct background checks, both initial and on-going, of personnel and vendors relevant to the registry services under application for criminal history, fiduciary conflicts of interest, fraudulent bona fides, and indicators of current or potential corruption?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.13. DDOS

Describe the solutions and mitigations to be used to thwart Distributed Denial of Service (DDOS) attacks.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.1.14. BCP 38

Does or will this RSP comply with BCP 38?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.1.15. Secure Routing

Does or will this RSP implement routing security of some nature, such as automated route filters, RPKI route origin validation, or other operational practices defined by the Internet Society's Mutually Agreed Norms for Routing Security (MANRS)?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2. Technical Overview

Provide a technical overview of the systems, software, and technical practices of the registry service provider.

Provide answers for the following:

DNSSEC.2.1. Systems and Software

Describe the systems and software relating to the operation of the RSP and the purpose and function for each. This must include, but is not limited to, types of operating systems, application software, programming languages, virtualization environments, network elements, appliances, and sizing requirements. The given list must contain software and systems which are both modern and in common use.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.2.2. Standard Hardware Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.3. Standard Hardware Lifecycle

Does or will this RSP have documented, regular, and active practices for the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.4. Standard Hardware Lifecycle

Does or will this RSP have documented, regular, and active practices for the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.5. Secure Software Development

Does or will this RSP have documented, regular, and active practices for the secure development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.6. Hardware Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.7. Software Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.

- This is a sub-question common to all types of RSP.

DNSSEC.2.8. Hardware Lifecycle Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.9. Software Development Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.10. IaC

Does or will this RSP use Infrastructure-as-Code (IaC) to manage all systems relevant to operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.2.11. Automated Orchestration

Does or will this RSP use automated orchestration to manage all systems relevant to the operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.3. Architecture

Provide answers for the following:

DNSSEC.3.1. Network Architecture

Describe the network architecture relevant to the registry services under application. This includes, but is not limited to, descriptions of network segmentation, interior and exterior routing schemes, virtual private networks, and IP addressing plans.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

DNSSEC.3.2. Fault Tolerance

Describe the methods for resiliency of servers, including the use of load balancers, proxies, reverse proxies, caches, and other network elements.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

DNSSEC.3.3. Tier III Data Center

Does or will this RSP have at least two Tier III (as defined here: https://uptimeinstitute.com/tiers) or equivalent data centers having no inter-dependencies?

- Answer format: Yes or No.
- This answer must include an attachment of the certification or equivalent documentation in either JPG, PNG, or PDF format.
- Relevant Link: [Uptime Institute](https://uptimeinstitute.com/tiers)

DNSSEC.3.4. Zone Resiliency

Describe the methods providing resiliency for DNSSEC, including the use of hidden DNS zone transfer servers.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNSSEC.3.5. DNSSEC to DNS Data Transfer

Describe the data transfer between DNS signing services and infrastructure to DNS authoritative servers, whether in-house or third-party (i.e. DNSSEC RSP -> DNS RSP).

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNSSEC.3.6. SRS to DNSSEC Data Transfer

Describe the data transfer from the SRS to the DNSSEC signing infrastructure, whether in-house or third-party (i.e. Main RSP -> DNSSEC RSP).

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNSSEC.3.7. Signing Performance

Provide the peak and sustained signing performance of the DNS signing infrastructure, and describe the methods used to collect this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNSSEC.3.8. Cryptographic Hardware and Software

Describe the hardware and software used to secure cryptographic material, cryptographic key escrow management, and hardware failover mechanisms related to DNSSEC services.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).

DNSSEC.3.9. FIPS 140-3

Does or will this RSP use hardware security modules (HSMs) certified to at least FIPS 140-3?

- Answer format: Yes or No.

DNSSEC.4. DNSSEC Capabilities

Describe the nature, architecture, and operation of nameservers and DNSSEC service, including compliance with the relevant DNS and DNSSEC standards.

Provide answers for the following:

DNSSEC.4.1. DPS

Provide the DNSSEC Policy and Practice Statement (DPS) to be used, in addition to any other relevant information regarding the handling and maintenance of DNSSEC cryptographic key material.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).

- This answer must include an attachment of the DPS in either PNG, JPG, or PDF format.

DNSSEC.4.2. Signing Infrastructure

Descriptions of the architecture and operation of DNSSEC signing infrastructure.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

DNSSEC.4.3. RFC 4033

Does or will this RSP implement RFC 4033 (“DNS Security Introduction and Requirements”)?

- Answer format: Yes or No.

DNSSEC.4.4. RFC 4034

Does or will this RSP implement RFC 4034 (“Resource Records for the DNS Security Extensions”)?

- Answer format: Yes or No.

DNSSEC.4.5. RFC 4035

Does or will this RSP implement RFC 4035 (“Protocol Modifications for the DNS Security Extensions”)?

- Answer format: Yes or No.

DNSSEC.4.6. RFC 4509

Does or will this RSP implement RFC 4509 (“Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)”)?

- Answer format: Yes or No.

DNSSEC.4.7. RFC 6840

Does or will this RSP implement RFC 6840 (“Clarifications and Implementation Notes for DNS Security (DNSSEC)”)?

- Answer format: Yes or No.

DNSSEC.4.8. RFC 6781

Does or will this RSP implement RFC 6781 (“DNSSEC Operational Practices, Version 2”)?

- Answer format: Yes or No.

DNSSEC.4.9. RFC 7583

Does or will this RSP implement RFC 7583 (“DNSSEC Key Rollover Timing Considerations”)?

- Answer format: Yes or No.

DNSSEC.4.10. RFC 9276

Does or will this RSP implement RFC 9276 (“Guidance for NSEC3 Parameter Settings”)?

- Answer format: Yes or No.

DNSSEC.4.11. RFCs 6605, 5702, and 8080

Does or will this RSP implement any of RFC 6605 (“Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC”), RFC 5702 (“Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC“), and/or RFC 8080 (“Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC”)?

- Answer format: Yes or No.

DNSSEC.4.12. DNSSEC Performance

Provide the peak and sustained DNSSEC signing operations, including measurements for both incremental and full zone updates and the methods used for each. Describe the methods used to obtain these measurements.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

DNSSEC.4.13. DNSSEC Fault Tolerance

Describe the fault tolerance methods used by the DNSSEC signing infrastructure and zone signature consistency as it applies to failure scenarios.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

DNSSEC.4.14. DNSSEC Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the DNSSEC service in such a manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to DNSSEC (excluding system services such as monitoring, remote access NTP)?

- Answer format: Yes or No.

DNSSEC.5. Registry Continuity

Describe how the registry service provider will comply with registry continuity, including but not limited to obligations as described in Specification 6 (section 3) to the Registry Agreement. This includes conducting registry operations using diverse, redundant servers to ensure continued operation of critical functions in the case of technical failure.

Provide answers for the following:

DNSSEC.5.1. Registry Continuity Exercise

Does or will this RSP regularly exercise registry continuity actions?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.5.2. Registry Continuity Compliance

Describe how this RSP will be in compliance with Specification 6.3 of the ICANN Registry Agreement.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.5.3. EBERO

Does or will this RSP participate in coordinated Emergency Back-end Registry Operator (EBERO) transitions, including but not limited to maintaining the DNSSEC chain of trust, of hosted gTLDs when the business relationship of this RSP and the Registry Operator is not in good standing?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6. Monitoring and Fault Escalation Processes

Describe arrangements for monitoring critical registry systems (including DNS security services, network connectivity, routers and firewalls). This description should explain how these systems are monitored and the mechanisms that will be used for fault escalation and reporting, and should provide details of the proposed support arrangements for these registry systems.

Provide answers for the following:

DNSSEC.6.1. Internal Monitoring

Does or will this RSP monitor for faults inside its own network?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.2. External Monitoring

Does or will this RSP monitor for faults from a point outside any of its own networks?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.3. Fault Triage

Does or will this RSP have documented processes for aggregation and triage of faults?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.4. Fault Mitigation

Does or will this RSP have documented processes to mitigate faults once detected?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.5. Regional Points of Presense

Provide a list of at least one point of presence where fault monitoring is conducted from each of the continents of North America, Central or South America, Asia, Europe, and Africa.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.6.6. Fault Minimization

Does or will this RSP have processes to minimize faults during maintenance of systems, including both automated processes and manual change control processes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.7. On-call Staff

Does or will this RSP have personnel capable of reacting to and mitigating faults 24 hours per day of every day of every year of service?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

DNSSEC.6.8. Service Disruptions

Provide documentation regarding any RSP functions currently being served for any gTLD, the domain names of the gTLDs, and all service disruptions for each gTLD in the past six months, where a service disruption is defined by Specification 10 of the Registry Agreement).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.6.9. Zone Pipelines

Describe the processes to insure accurate, complete and compliant DNS zones such as staged roll-outs, zone pipelines, and other quality assurance methodologies.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

DNSSEC.7. Capacity

Provide a summary of capacity capabilities and other information necessary for the adequate approval of the RSP to accommodate the projected forecast of gTLD(s). The Main RSP should at least support the aggregate of the expected number of domain names within 3 years for all TLDs using the RSP plus the currently supported TLDs, if any.

Provide answers for the following:

DNSSEC.7.1. DUMs per TLD

Provide the maximum number of Domains Under Management (DUMs) per TLD, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.7.2. Maximum TLDs

Provide the maximum number of TLDs that may be serviced, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.7.3. Current DUMs

Provide the current TLDs being serviced and the DUMs for each, if any.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.7.4. Maximum Capacity

Provide the maximum number of TLDs and combined DUMs that can be serviced from the least-capable data center. If service is provided using public cloud services, provide the maximum capacity based on the contracted resources. Describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

DNSSEC.7.5. Available Load

Provide documentation that either services contracted from a public cloud provider or services provided from private sources demonstrate the needed capacity as stated above. This documentation may include, but is not limited to, number of servers, contracted bandwidth from network providers, and load test reports.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

- This is a sub-question common to all types of RSP.

Proxy RSP

A Proxy RSP is responsible for operating an RSP in a designated jurisdiction. Proxy RSPs must adhere to regulations and legislation of that jurisdiction, while also ensuring that any infrastructure deployed in that jurisdiction operates in accordance with the relevant specifications from the Registry Agreement.

A Proxy RSP operates EPP and RDAP services under the applicable laws of the jurisdiction and sends domain registrations to a Main RSP. A Proxy RSP also operates a proxy RDAP service for a Main RSP under the applicable laws of the jurisdiction.

PROXY.1. Security Controls

Provide a summary of the security controls for the proposed registry service provider, encompassing both physical security and logical security regarding the operation of gTLD registry services. This information applies to in-house and all third-party (e.g. cloud providers, software vendors) vendors relevant to the registry services under application.

Provide answers for the following:

PROXY.1.1. Third-Party Certificate

Does or will this RSP have a publicly verifiable, 3rd party certification (e.g. ISO 27001) held directly by the organization and relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.2. Information Security Management System

Describe the information security management system (ISMS) implemented by this RSP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.1.3. Physical Access Controls

Does or will this RSP have processes and controls to manage physical access to infrastructure and systems, including building access controls, security cameras and/or

other sensors, physical environmental monitoring and safety equipment, and alarm systems related to the physical infrastructure?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.4. System Access Controls

Does or will this RSP have processes and controls to manage non-physical access to infrastructure, including network access from both internal systems and external Internet systems, intrusion detection systems, security information and event management systems, network firewalls, network segmentation and isolation, user identification and authentication, and authorization schemes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.5. Vendor Management

Does or will this RSP have processes and controls pertaining to the selection of vendors and equipment suppliers, management and maintenance of assets while in use, procurement of assets, and safe disposal of assets?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.6. Cryptographic Material

Does or will this RSP routinely renew and keep safe all cryptographic material necessary for the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.7. Secure Data At-Rest

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) at-rest data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.8. Secure Data In-Transit

Does or will this RSP secure (e.g. encryption, tamper detection, etc…) in-transit data relevant to the operation of the RSP, including but not limited to DNSSEC if applicable?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.9. Virtualization Controls

If applicable, does or will this RSP have security controls for data in virtualized environments, including controls relevant to both on-premises or private virtualization environments as well as public clouds, network isolation, memory isolation, process isolation, and hypervisor access controls?

- Answer format: Yes, No, or Not Applicable.
- This is a sub-question common to all types of RSP.

PROXY.1.10. CISO

Does or will this RSP have a senior executive primarily in charge of and responsible for security?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.11. Emerging Threats

Describe the dedicated resources used to address emerging threats. This includes, but is not limited to, the utilization of either an in-house or third-party Computer Emergency Response Team (CERT), penetration testing schedule, software supply chain scanning, and participation in DNS, network, and/or security related forums (e.g. NANOG, RIPE, DNS-OARC).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.1.12. Background Checks

Does or will this RSP conduct background checks, both initial and on-going, of personnel and vendors relevant to the registry services under application for criminal history, fiduciary conflicts of interest, fraudulent bona fides, and indicators of current or potential corruption?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.13. DDOS

Describe the solutions and mitigations to be used to thwart Distributed Denial of Service (DDOS) attacks.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

- This is a sub-question common to all types of RSP.

PROXY.1.14. BCP 38

Does or will this RSP implement BCP 38?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.1.15. Secure Routing

Does or will this RSP implement routing security of some nature, such as automated route filters, RPKI route origin validation, or other operational practices defined by the Internet Society's Mutually Agreed Norms for Routing Security (MANRS)?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2. Technical Overview

Provide a technical overview of the systems, software, and technical practices of the registry service provider.

Provide answers for the following:

PROXY.2.1. Systems and Software

Describe the systems and software relating to the operation of the RSP and the purpose and function for each. This must include, but is not limited to, types of operating systems, application software, programming languages, virtualization environments, network elements, appliances, and sizing requirements. The given list must contain software and systems which are both modern and in common use.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This is a sub-question common to all types of RSP.

PROXY.2.2. Standard Hardware Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.3. Standard Software Maintenance

Does or will this RSP have documented, regular, and active practices for the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.4. Standard Hardware Lifecycle

Does or will this RSP have documented, regular, and active practices for the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.5. Secure Software Development

Does or will this RSP have documented, regular, and active practices for the secure development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.6. Hardware Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance of hardware relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.7. Software Maintenance Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the maintenance, upgrading, and patching of software relevant to the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.8. Hardware Lifecycle Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the lifecycle of hardware relevant to the registry services under application?

- Answer format: Yes or No.

- This is a sub-question common to all types of RSP.

PROXY.2.9. Software Development Contingency

Does or will this RSP have documented contingency plans for extraordinary scenarios regarding the development of software?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.10. IaC

Does or will this RSP use Infrastructure-as-Code (IaC) to manage all systems relevant to operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.2.11. Automated Orchestration

Does or will this RSP use automated orchestration to manage all systems relevant to the operation of the registry services under application?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY..3. Architecture

Provide an architectural overview of the systems and software of the registry service provider, including descriptions of software architecture, systems dependencies, data flow within the registry, and logical systems interconnections.

Provide answers for the following:

PROXY.3.1. Network Architecture

Describe the network architecture relevant to the registry services under application. This includes, but is not limited to, descriptions of network segmentation, interior and exterior routing schemes, virtual private networks, and IP addressing plans.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

PROXY.3.2. Fault Tolerance

Describe the methods for resiliency of servers, including the use of load balancers, proxies, reverse proxies, caches, and other network elements.

- The answer to this question will not be published.
- Answer format: free text of no more than 12000 characters (approx. 4 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.
- This is a sub-question common to all types of RSP.

PROXY.3.3. Tier III Data Center

Does or will this RSP have at least two Tier III (as defined here: https://uptimeinstitute.com/tiers) or equivalent data centers having no inter-dependencies?

- Answer format: Yes or No.
- This answer must include an attachment of the certification or equivalent documentation in either JPG, PNG, or PDF format.
- Relevant Link: [Uptime Institute](https://uptimeinstitute.com/tiers)

PROXY.4. EPP Service

Describe the use of the Extensible Provisioning Protocol (EPP) by the registry service provider. Provide details on usage of EPP extensions, performance characteristics, security controls to be used with EPP, and other technical details.

Provide answers for the following:

PROXY.4.1. RFC 5730

Does or will this RSP implement RFC 5730 (“Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes or No.

PROXY.4.2. RFC 5731

Does or will this RSP implement RFC 5731 (“Extensible Provisioning Protocol (EPP) Domain Name Mapping”)?

- Answer format: Yes or No.

PROXY.4.3. RFC 5734

Does or will this RSP implement RFC 5734 (“Extensible Provisioning Protocol (EPP) Transport over TCP”)?

- Answer format: Yes or No.

PROXY.4.4. RFC 5910

Does or will this RSP implement RFC 5910 (“Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes or No.

PROXY.4.5. RFC 5733

If applicable, does or will this RSP implement RFC 5733 (“Extensible Provisioning Protocol (EPP) Contact Mapping”)?

- Answer format: Yes, No, or Not Applicable.

PROXY.4.6. RFC 8334

If applicable, does or will this RSP implement RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”)?

- Answer format: Yes, No, or Not Applicable.

PROXY.4.7. RFC 8334 Mechanisms

If RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”) is not applicable to this RSP, describe the mechanism to support sunrise and claims in EPP. Please answer with “Not Applicable” or “N/A” if this RSP does or will implement RFC 8334.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- Note that this question does not need to be answered if the RSP does implement RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”). See sub-question above.

PROXY.4.8. EPP Extensions

Provide a list of all EPP extensions to be used that are registered in the IANA EPP extensions registry, and an attestation that all EPP extensions to be used are registered with the IANA as per RFC 7451 (“Extension Registry for the Extensible Provisioning Protocol”).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.4.9. Unregistered EPP Extensions

Does or will this RSP forgo the use of any EPP extensions which are not registered with the IANA as per RFC 7451 (“Extension Registry for the Extensible Provisioning Protocol”)?

- Answer format: Yes or No.

PROXY.4.10. EPP Performance

Does or will this RSP implement and operate EPP according to the performance requirements defined in Specification 10 of the ICANN Registry Agreement?

- Answer format: Yes or No.

PROXY.4.11. EPP Equal Access

Does or will this RSP have controls to prevent EPP misuse and ensure all registrars have fair and equal access to EPP per Specification 9 of the ICANN Registry Agreement?

- Answer format: Yes or No.

PROXY.4.12. EPP Client Connections

Describe how data integrity is achieved across multiple client connections, including but not limited to usage of soft-state and eventual consistency if applicable, and the application of Atomicity, Consistency, Isolation, and Durability (ACID) principles.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.4.13. EPP 9325

Does or will this RSP implement RFC 9325 (“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”) notwithstanding RFC 5734 (“Extensible Provisioning Protocol (EPP) Transport over TCP”)?

- Answer format: Yes or No.

PROXY.4.14. EPP Cryptographic Material Renewal

Does or will this RSP regularly and frequently renew the cryptographic material used to secure EPP communications in accordance with industry best common practices?

- Answer format: Yes or No.

PROXY.4.15. EPP Cryptographic Material Handling

Does or will this RSP keep safe the cryptographic material used to secure EPP communication in accordance with industry best common practices?

- Answer format: Yes or No.

PROXY.4.16. EPP Reporting

Does or will this RSP comply with Specification 3 of the ICANN Registry Agreement with respect to EPP?

- Answer format: Yes or No.

PROXY.4.17. EPP Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the EPP service in such a manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to EPP (excluding system services such as monitoring, remote access and NTP)?

- Answer format: Yes or No.

PROXY.5. RDAP

Describe the use of the Registration Data Access Protocol (RDAP) by the registry service provider. Provide details on usage of RDAP extensions, performance characteristics, security controls to be used with RDAP, and other technical details.

Provide answers for the following:

PROXY.5.1. RFC 7480

Does or will this RSP implement RFC 7480 (“HTTP Usage in the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

PROXY.5.2. RFC 7481

Does or will this RSP implement RFC 7481 (“Security Services for the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

PROXY.5.3. RFC 9082

Does or will this RSP implement RFC 9082 (“Registration Data Access Protocol (RDAP) Query Format”)?

- Answer format: Yes or No.

PROXY.5.4. RFC 9083

Does or will this RSP implement RFC 9083 (“JSON Responses for the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

PROXY.5.5. RDAP Technical Implementation Guide

Does or will this RSP implement the ICANN gTLD RDAP Technical Implementation Guide?

- Answer format: Yes or No.

PROXY.5.6. RDAP Response Profile

Does or will this RSP implement the ICANN gTLD RDAP Response Profile?

- Answer format: Yes or No.

PROXY.5.7. RDAP Extensions

Provide a list of all RDAP extensions to be used.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.5.8. Unregistered RDAP Extensions

Does or will this RSP forgo the use of any RDAP extensions which are not registered with the IANA as per RFC 7480 (“HTTP Usage in the Registration Data Access Protocol (RDAP)”)?

- Answer format: Yes or No.

PROXY.5.9. RDAP Performance

Does or will this RSP comply with the Service Level Agreements of the ICANN Registry Agreement (Specification 10) with regard to RDAP?

- Answer format: Yes or No.

PROXY.5.10. RDAP Data Mining

Does or will this RSP implement methods to prevent mining of registration data via RDAP?

- Answer format: Yes or No.

PROXY.5.11. RFC 9325

Does or will this RSP implement RFC 9325 (“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”) with respect to RDAP?

- Answer format: Yes or No.

PROXY.5.12. RFC Cryptographic Material Renewal

Does or will this RSP regularly and frequently renew the cryptographic material used to secure RDAP communications in accordance with industry best common practices?

- Answer format: Yes or No.

PROXY.5.13. RFC Cryptographic Material Handling

Does or will this RSP keep safe the cryptographic material used to secure RDAP communication in accordance with industry best common practices?

- Answer format: Yes or No.

PROXY.5.14. RDAP Reporting

Does or will this RSP comply with Specification 3 of the ICANN Registry Agreement with respect to RDAP?

- Answer format: Yes or No.

PROXY.5.15. RDAP Virtualization

Does or will this RSP compartmentalize (e.g. virtualization) the RDAP service in such a manner that each compartment (e.g. containers, virtual machines, physical machines) is dedicated to RDAP (excluding system services such as monitoring, remote access and NTP)?

- Answer format: Yes or No.

PROXY.6. Internet Connectivity

Describe the IPv4 and IPv6 connectivity and reachability of the registry service provider, including performance characteristics, transit, cloud, and/or backbone providers, peering exchanges, routing stability and other information.

Provide answers for the following:

PROXY.6.1. IPv4 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv4 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.6.2. IPv6 Connectivity

Provide a list of the transit, cloud, backbone, and network providers and points of presence through which IPv6 services are to be provided, including egress and ingress data transfer speeds.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.6.3. IPv4 RDAP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to RDAP and IPv4?

- Answer format: Yes or No.

PROXY.6.4. IPv4 EPP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to EPP and IPv4?

- Answer format: Yes or No.

PROXY.6.5. IPv6 RDAP

Does or will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to RDAP and IPv6?

- Answer format: Yes or No.

PROXY.6.6. IPv6 EPP

Will this RSP comply with Specification 10 of the ICANN Registry Agreement with regard to EPP and IPv6 if requested by a registrar?

- Answer format: Yes or No.

PROXY.7. Registration Lifecycle

Provide a detailed description of the proposed registration lifecycle for domain names. Explain the various registration states, state transition timelines, and relationship of these states with EPP and RDAP.

Provide answers for the following:

PROXY.7.1. Registration Lifecycle

Describe all potential registration lifecycle(s) of domain names supported in the system.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include attachments of diagrams in either PNG, JPG, or PDF format.

PROXY.7.2. Domain Registration Values

Describe the registration lifecycle(s) of domain names with respect to EPP status values and RDAP status values.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.7.3. Nameserver Registration Values

Describe the nameserver host lifecycle, including relevance to EPP and RDAP status values, with respect to the lifecycle of domain names. This should include a description of nameservers as either attributes of domains or as host objects.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.7.4. Contact Registration Values

If applicable, describe the contact lifecycle, including relevance to EPP and RDAP status values, with respect to the lifecycle of domain names and nameservers. Include a description of the deletion of orphaned contacts.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.7.5. Orphaned Glue

Does or will this RSP be capable of removing orphaned glue in accordance with Specification 6 of the ICANN Registry Agreement?

- Answer format: Yes, No, or Not Applicable.

PROXY.7.6. BRDA

Describe the systems, software, and processes used to integrate to ICANN's Bulk Registration Data Access (BRDA, Specification 4 of the Registry Agreement), ICANN's Registration Reporting System (RRI, Specification 2 and Specification 3 of the Registry Agreement), and ICANN's Zone File Access (ZFA, Specification 4 of the Registry Agreement).

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.7.7. Data Escrow

Describe how this RSP will comply with Specification 2 of the Registry Agreement, and describe any other data escrow processes. This includes escrow extensions for data related additional registry services.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

PROXY.8. Registry Continuity

Describe how the registry service provider will comply with registry continuity, including but not limited to obligations as described in Specification 6 (section 3) to the Registry Agreement. This includes conducting registry operations using diverse, redundant servers to ensure continued operation of critical functions in the case of technical failure.

Provide answers for the following:

PROXY.8.1. Registry Continuity Exercise

Does or will this RSP regularly exercise registry continuity actions?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.8.2. Registry Continuity Compliance

Describe how this RSP will be in compliance with Specification 6.3 of the ICANN Registry Agreement.

- The answer to this question will not be published.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.9. Monitoring and Fault Escalation

Describe arrangements for monitoring critical registry systems (including SRS, database systems, EPP services, RDAP services, network connectivity, routers and firewalls). This description should explain how these systems are monitored and the mechanisms that will be used for fault escalation and reporting, and should provide details of the proposed support arrangements for these registry systems.

Provide answers for the following:

PROXY.9.1. Internal Monitoring

Does or will this RSP monitor for faults inside its own network?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.2. External Monitoring

Does or will this RSP monitor for faults from a point outside any of its own networks?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.3. Fault Triage

Does or will this RSP have documented processes for aggregation and triage of faults?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.4. Fault Mitigation

Does or will this RSP have documented processes to mitigate faults once detected?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.5. Fault Minimization

Does or will this RSP have processes to minimize faults during maintenance of systems, including both automated processes and manual change control processes?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.6. On-call Staff

Does or will this RSP have personnel capable of reacting to and mitigating faults 24 hours per day of every day of every year of service?

- Answer format: Yes or No.
- This is a sub-question common to all types of RSP.

PROXY.9.7. Service Disruptions

Provide documentation regarding any RSP functions currently being served for any gTLD, the domain names of the gTLDs, and all service disruptions for each gTLD in the past six months, where a service disruption is defined by Specification 10 of the Registry Agreement).

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.10. Capacity

Provide a summary of capacity capabilities and other information necessary for the adequate approval of the RSP to accommodate the projected forecast of gTLD(s).

Provide answers for the following:

PROXY.10.1. DUMs per TLD

Provide the maximum number of Domains Under Management (DUMs) per TLD, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.10.2. Maximum TLDs

Provide the maximum number of TLDs that may be serviced, and describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.10.3. Current TLDs

Provide the current TLDs being serviced and the DUMs for each, if any.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.10.4. Maximum Capacity

Provide the maximum number of TLDs and combined DUMs that can be serviced from the least-capable data center. If service is provided using public cloud services, provide the maximum capacity based on the contracted resources. Describe the methods used to determine this information.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

PROXY.10.5. Available Load

Provide documentation that either services contracted from a public cloud provider or services provided from private sources demonstrate the needed capacity as stated above. This documentation may include, but is not limited to, number of servers, contracted bandwidth from network providers, and load test reports.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This is a sub-question common to all types of RSP.

Appendix B. IDN Services Application Technical Questions

A Main RSP may apply to support IDN services based on support for variant TLDs and support for variant IDNs in the second-level. IDN services are denoted by three support levels as defined in 4.1.12. Internationalized Domain Name (IDN) Evaluation.

Applicants will be required to answer technical questions appropriate to the level of service selected.

IDN.1. Level 1 Questions

Provide answers to the following:

IDN.1.1. IDN Guidelines

Does or will the RSP implement the IDN Guidelines 4.1?

- Answer format: Yes or No.

- Relevant Link: [IDN Guidelines 4.1](https://www.icann.org/en/system/files/files/idn-guidelines-22sep22-en.pdf)

IDN.1.2. Architecture

Describe the software architecture, systems dependencies, data flow with the registry, and logical systems interconnections for supporting the following: a) IDN validation with IDNA2008, b) IDN tables, c) IDN provisioning via EPP, and d) datastore capabilities.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

IDN.2. Level 2 Questions

Provide answers to the following:

IDN.2.1. IDN Guidelines

Does or will the RSP implement the IDN Guidelines 4.1?

- Answer format: Yes or No.
- Relevant Link: [IDN Guidelines 4.1](https://www.icann.org/en/system/files/files/idn-guidelines-22sep22-en.pdf)

IDN.2.2. Architecture

Describe the software architecture, systems dependencies, data flow with the registry, and logical systems interconnections for supporting the following: a) IDN validation with IDNA2008, b) IDN tables, c) IDN provisioning via EPP, and d) datastore capabilities.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

IDN.2.3. Second Level IDN Support

Describe the software architecture, systems dependencies, data flow within the registry, and logical systems interconnections for supporting variant IDNs at the second-level. This information should include a) the method(s) used to calculate variants, b) registration lifecycle of variants including primary/source names, c) lookup of IDN variants in RDAP, and d) variant management in EPP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

IDN.2.4. Same Entity Allocation

Describe how compliance will be achieved for second-level variant labels that arise from a registration based on a second-level IDN table where all allocatable variant labels in the set must only be allocated to the same entity or withheld for possible allocation only to that entity (e.g., all allocatable second-level labels {s1, s1v1, …} under the TLD.

Note: if the RSP will support a minimal registration data set as defined in the Registration Data Consensus Policy for gTLDs, please explain how this RSP will comply with the requirement in this section for minimal and full registration data sets. A contractual control may be acceptable to comply with this section in case of a minimal registration data set.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

IDN.3. Level 3 Questions

Provide answers to the following:

IDN.3.1. IDN Guidelines

Does or will the RSP implement the IDN Guidelines 4.1?

- Answer format: Yes or No.
- Relevant Link: [IDN Guidelines 4.1](https://www.icann.org/en/system/files/files/idn-guidelines-22sep22-en.pdf)

IDN.3.2. Architecture

Describe the software architecture, systems dependencies, data flow with the registry, and logical systems interconnections for supporting the following: a) IDN validation with IDNA2008, b) IDN tables, c) IDN provisioning via EPP, and d) datastore capabilities.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

IDN.3.3. Second Level IDN Support

Describe the software architecture, systems dependencies, data flow within the registry, and logical systems interconnections for supporting variant IDNs at the second-level under all allocated variant TLD labels. This information should include a) the method(s) used to calculate variants, b) registration lifecycle of variants including primary/source

names under all allocated variant TLD labels, c) lookup of IDN variants in RDAP, and d) variant management in EPP.

- The answer to this question will not be published.
- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer must include diagrams in either PNG, JPG, or PDF format.

IDN.3.4. Variant TLDs

Does or will this RSP support different set IDN tables under different variant TLDs (see 25.8 of the Final Report on the new gTLD Subsequent ProceduresPolicy Development Process)? For example, offering Spanish and Portuguese in TLD A, and only Spanish for TLD B, and TLD B is a variant of TLD A.

- Answer format: Yes or No.
- Relevant Link: [Final Report on the new gTLD Subsequent Procedures Policy Development Process](https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-02feb21-en.pdf)

IDN.3.5. Same Entity Allocation

Describe how this RSP's implementation will comply with the following: For second-level variant labels that arise from a registration based on a second-level IDN table, all allocatable variant labels in the set must only be allocated to the same entity or withheld for possible allocation only to that entity (e.g., all allocatable second-level labels {s1, s1v1, …} under all allocated variant TLD labels.

Note: if the RSP will support a minimal registration data set as defined in the Registration Data Consensus Policy for gTLDs, please explain how this RSP will comply with the requirement in this section for minimal and full registration data sets. A contractual control may be acceptable to comply with this section in case of a minimal registration data set.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

Appendix C. Registry Services Application Questions

The RSP Portal will have facilities for Main RSP applicants to add additional Registry Services to be offered by the RSP to Registry Operators as defined in 4.1.11. Registry Services Evaluation.

Applicants will be required to answer technical questions appropriate to the type of evaluation of the Registry Service.

RS.1. Existing Registry Services

Applicants currently operating Registry Services for a gTLD may apply to offer those Registry Services with their Main RSP to Registry Operators.

Provide answers for the following:

RS.1.1. Service Name

Please specify the name of the Registry Service.

- Answer format: free text of no more than 500 characters.

RS.1.2. Approved gTLDs

Please specify all gTLDs for which you are the RSP where the service is currently approved and specified in the Registry Agreement.

- Answer format: free text of no more than 500 characters.

RS.1.3. Service Description

Please provide the proposed language that describes the service. By providing this language, the RSP agrees to notify gTLD applicants that this language will be used in the Registry Agreement if the service is supported in the gTLD. Free text; 6,000 characters

Note: if the description of the service is materially different from the language in the registry agreement of the gTLDs listed in question 1, the proposed service will need to undergo full registry services evaluation.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2. New Registry Services

Applicants may apply to offer Registry Services that they currently do not offer for a gTLD or are not Fast Track Registry Services.

RS.2.1. Proposed Service Description

Provide answers for the following:

RS.2.1.1. Service Name

Name of proposed service.

- Answer format: free text of no more than 100 characters.

RS.2.1.2. Service Description

Provide a general description of the proposed service including the impact to external users and how it will be offered.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.1.3. Technical Description

Provide a technical description of the proposed service.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.1.4. Currently Approved RSEP

If this proposed service has already been approved by ICANN org for any gTLD, identify and provide a link to the RSEP request for the same service that was most recently approved..

- Answer format: free text of no more than 1000 characters.

RS.2.1.5. Service Benefits

Describe the benefits of the proposed service and who would benefit from the proposed service.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.1.6. Additional Information

If additional information should be considered with the description of the proposed service, elaborate or attach one or more file(s) below.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer may have optional attachments in either PNG, JPG, or PDF format

RS.2.2. Security and Stability

Provide answers for the following:

RS.2.2.1. Domain Lifecycle

What effect, if any, will the proposed service have on the life cycle of domain names?

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.2.2. Registration Data Storage

Does the proposed service alter the storage and input of Registry Data? If yes, please explain.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.2.3. Registration Performance

Explain how the proposed service will affect the throughput, response time, consistency or coherence of responses to Internet servers or end systems.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.2.4. Technical Concerns

Have technical concerns been raised about the proposed service? If so, identify the concerns and describe how you intend to address those concerns.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.2.5. Quality Assurance

Describe the quality assurance plan and/or testing of the proposed service prior to deployment.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.2.6. Relevant RFCs and White Papers

Identify and list any relevant RFCs or White Papers on the proposed service and explain how those papers are relevant.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.3. Contractual Provisions

Provide answers to the following:

RS.2.3.1. Relevant Contractual Provisions

List the relevant contractual provisions impacted by the proposed service necessary for a Registry Operator to use this proposed registry service. This includes, but is not limited

to, Consensus Policies, previously approved amendments or services, Reserved Names, and Rights Protection Mechanisms.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.3.2. Reporting Impact

What effect, if any, will the proposed service have upon a Registry Operator in regard to the reporting of data to ICANN?

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.3.3. RDDS Impact

What effect, if any, will the proposed service have upon a Registry Operator in regard to Registration Data Directory Service (RDDS)?

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.4. Authorization Language

Provide answers to the following:

RS.2.4.1. RA Amendment

A Registry Agreement (RA) amendment is required when the proposed service: (i) contradicts existing provisions in the RA or (ii) is not contemplated in the RA and, therefore, needs to be added to Exhibit A of the RA and/or as an appropriate addendum/appendix. If applicable, provide draft language (or a link to previously approved RA amendment language) describing the service to be used by a Registry Operator in an RA amendment if the proposed service is approved. If an RA amendment is not applicable, respond with “N/A” and provide a complete response to question 4.2.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.4.2. RA Provisions

If the proposed service is permissible under an existing provision in the Registry Agreement, identify the provision and provide rationale. If not applicable, respond with “N/A” and provide a complete response to question 4.1.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.5. Consultation

Provide answers to the following:

RS.2.5.1. Community Feedback

Describe your consultations with the community, experts, and/or others. This can include, but is not limited to, the relevant community for a sponsored or community TLD, registrars or the registrar constituency, end users and/or registrants, or other constituency groups. What were the quantity, nature, and results of the consultations? How will the proposed service impact these groups? Which groups support or oppose this proposed service?

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.6. Other

Provide answers to the following:

RS.2.6.1. Intellectual Property Considerations

Would there be any intellectual property impact or considerations raised by the proposed service? If so, please describe them.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.6.2. Exclusive Intellectual Property

Does the proposed service contain intellectual property exclusive to you? If so, please describe them.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.6.3. Other Relevant Information

Provide any other relevant information to include with the request. If none, respond with “N/A.”

- Answer format: free text of no more than 6000 characters (approx. 2 pages).

RS.2.6.4. Additional Information

If additional information should be considered, elaborate or attach one or more file(s) below.

- Answer format: free text of no more than 6000 characters (approx. 2 pages).
- This answer may have optional attachments in either PNG, JPG, or PDF format.