Proxy RSP Technical Evaluation Questionnaire

The questions provided in this document will be incorporated into the RSP Evaluation Program Handbook to be provided to applicants in advance of the start of the application period. These questions 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.

This document only covers the technical questionnaire for the Proxy RSP (4) type. Main RSP (1), DNS RSP (2), and DNSSEC RSP (3) are covered in other documents

Depending on the sub-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.

4. 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.

4.1. 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:

a. Provide a list of all security assessments having received publicly verifiable, 3rd party certification (e.g. ISO 27001) held by the organization and relevant to the registry services under application. For assessments relevant to in-house processes, infrastructure, and systems, specify (a) the year and month the assessment was first

conducted or attained, (b) the year and month of the most recent renewal of the assessment (if applicable), (c) the year and month of next planned renewal of the assessment (if applicable), and (d) a URL or some other identifying information or attachment to be used to verify this information. For assessments relevant to third-party vendors (e.g. cloud providers), specify (a) the name of the vendor, (b) the service provided by the vendor, and (c) a URL to the assessment.

    - Answer format: free text of no more than 6000 characters (approx. 2 pages).
    - This is a sub-question common to all types of RSP.
    - This answer may have optional attachments in either PNG, JPG, or PDF format.

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

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

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. 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).

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

l. 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.

m. 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.

n. 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.

o. 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.

4.2. Technical Overview

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

Provide answers for the following:

a. 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.

   - Answer format: free text of no more than 12000 characters (approx. 4 pages).
   - This is a sub-question common to all types of RSP.

b. Does or will this RSP have normative, 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.

c. Does or will this RSP have normative, 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.

d. Does or will this RSP have normative, 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.

e. Does or will this RSP have normative, 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.

f. Does or will this RSP have normative and extra-ordinary 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.

g. Does or will this RSP have normative and extra-ordinary 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.

h. Does or will this RSP have normative and extra-ordinary 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.

i. Does or will this RSP have normative and extra-ordinary practices for the development of software?

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

j. 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.

k. 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.

4.3. 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:

a. 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.

    - 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.

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

    - 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.

c. 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.

4.4. 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:

a. Does or will this RSP comply with RFC 5730 (“Extensible Provisioning Protocol (EPP)”)?

    - Answer format: Yes or No.

b. Does or will this RSP comply with RFC 5731 (“Extensible Provisioning Protocol (EPP) Domain Name Mapping”)?

    - Answer format: Yes or No.

c. Does or will this RSP comply with RFC 5734 (“Extensible Provisioning Protocol (EPP) Transport over TCP”)?

    - Answer format: Yes or No.

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

    - Answer format: Yes or No.

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

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

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

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

g. 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.

    - 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 comply with RFC 8334 (“Launch Phase Mapping for the Extensible Provisioning Protocol (EPP)”). See sub-question above.

h. 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).

i. 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.

j. Provide the peak and sustained throughput for each of the “check”, “create”, “delete”, “info”, “update”, “transfer” and “renew” EPP commands for domain objects and, if applicable for host and contact objects, and describe the methods used to determine this information.

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

k. 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.

l. 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.

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

m. Does or will this RSP comply with 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.

n. 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.

o. 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.

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

    - Answer format: Yes or No.

q. 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.

4.5. 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:

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

    - Answer format: Yes or No.

b. Does or will this RSP comply with RFC 7481 (“Security Services for the Registration Data Access Protocol (RDAP)”)?
    - Answer format: Yes or No.
c. Does or will this RSP comply with RFC 8521 (“Registration Data Access Protocol (RDAP) Object Tagging”) for all currently operated gTLDs?
    - Answer format: Yes or No.
d. Does this RSP plan to continue to comply with RFC 8521 (“Registration Data Access Protocol (RDAP) Object Tagging”) for all gTLDs operated in the future?
    - Answer format: Yes or No.
e. Does or will this RSP comply with RFC 9082 (“Registration Data Access Protocol (RDAP) Query Format”)?
    - Answer format: Yes or No.
f. Does or will this RSP comply with RFC 9083 (“JSON Responses for the Registration Data Access Protocol (RDAP)”)?
    - Answer format: Yes or No.
g. Does or will this RSP comply with RFC 9224 (“Finding the Authoritative Registration Data Access Protocol (RDAP) Service”) for all currently operated gTLDs?
    - Answer format: Yes or No.
h. Will this RSP comply with RFC 9224 (“Finding the Authoritative Registration Data Access Protocol (RDAP) Service”) for all gTLDs operated in the future?
    - Answer format: Yes or No.
i. Does or will this RSP comply with the ICANN gTLD RDAP Technical Implementation Guide?
    - Answer format: Yes or No.
j. Does or will this RSP comply with the ICANN gTLD RDAP Response Profile?
    - Answer format: Yes or No.
k. Provide a list of all RDAP extensions to be used.
    - Answer format: free text of no more than 6000 characters (approx. 2 pages).

l. 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.

m. Provide the peak and sustained queries to RDAP for domains and, if applicable, nameservers and entities, and describe the methods used to determine this information.

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

n. 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.

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

    - Answer format: Yes or No.

p. Does or will this RSP comply with 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.

q. 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.

r. 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.

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

    - Answer format: Yes or No.

t. 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.

4.6. 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:

a. 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.
    - Answer format: free text of no more than 6000 characters (approx. 2 pages).
b. 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.
    - Answer format: free text of no more than 6000 characters (approx. 2 pages).
c. 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.
d. 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.
e. 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.
f. 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.

4.7. 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:

a. 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.

b. 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).

c. 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).

d. 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).

e. Does or will this RSP remove orphaned glue when provided with evidence in accordance with Specification 6 of the Registry Agreement?
    - Answer format: Yes or No.

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

g. 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).

4.8. 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:

a. 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.

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

4.9. 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:

a. 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.

b. 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.

c. Does or will this RSP have normative processes for aggregation and triage of faults?
    - Answer format: Yes or No.
    - This is a sub-question common to all types of RSP.

d. Does or will this RSP have normative processes to mitigate faults once detected?
    - Answer format: Yes or No.
    - This is a sub-question common to all types of RSP.

e. 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.

f. 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.

g. 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.

4.10. 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:

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

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

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

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

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

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

d. 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.

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

e. 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.

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