III. TECHNICAL QUESTIONS

If the proposed provider is not currently operating one or more New gTLD registries, provide attachment(s) including responses to each of the questions below. If the Material Subcontracting Arrangement request will not affect the response to a question or set of questions listed below, please indicate so in the response.

1. **SHARED REGISTRATION SYSTEM (SRS) PERFORMANCE: DESCRIBE**

   - The plan for operation of a robust and reliable SRS. SRS is a critical registry function for enabling multiple registrars to provide domain name registration services in the TLD. SRS must include the EPP interface to the registry, as well as any other interfaces intended to be provided, if they are critical to the functioning of the registry. Please refer to the requirements in Specification 6 (section 1.2) and Specification 10 (SLA Matrix) attached to the Registry Agreement; and
   - Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer should include, but is not limited to:

- A high-level SRS system description;
- Representative network diagram(s);
- Number of servers;
- Description of interconnectivity with other registry systems;
- Frequency of synchronization between servers; and
- Synchronization scheme (e.g., hot standby, cold standby).

2. **EXTENSIBLE PROVISIONING PROTOCOL (EPP): PROVIDE A DETAILED DESCRIPTION OF THE INTERFACE WITH REGISTRARS, INCLUDING HOW THE REGISTRY OPERATOR WILL COMPLY WITH EPP IN RFCS 3735 (IF APPLICABLE), AND 5730-5734.**

If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.
Describe resourcing plans (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

3. WHOIS: DESCRIBE

- How the Registry Operator will comply with Whois specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement;
- How the Registry Operator Whois service will comply with RFC 3912; and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer should include, but is not limited to:

- A high-level Whois system description;
- Relevant network diagram(s);
- IT and infrastructure resources (e.g., servers, switches, routers and other components);
- Description of interconnectivity with other registry systems; and
- Frequency of synchronization between servers.

Answers may also include:

- Provision for Searchable Whois capabilities; and
- A description of potential forms of abuse of this feature, how these risks will be mitigated, and the basis for these descriptions.

A complete answer is expected to be no more than 5 pages.

4. **REGISTRATION LIFE CYCLE:**
Provide a detailed description of the proposed registration lifecycle for domain names in the proposed gTLD. The description must:

- Explain the various registration states as well as the criteria and procedures that are used to change state;
- Describe the typical registration lifecycle of create/update/delete and all intervening steps such as pending, locked, expired, and transferred that may apply;
- Clearly explain any time elements that are involved - for instance details of add-grace or redemption grace periods, or notice periods for renewals or transfers; and
- Describe resourcing plans for this aspect of the criteria (number and description of personnel roles allocated to this area).

The description of the registration lifecycle should be supplemented by the inclusion of a state diagram, which captures definitions, explanations of trigger points, and transitions from state to state.

If applicable, provide definitions for aspects of the registration lifecycle that are not covered by standard EPP RFCs.

A complete answer is expected to be no more than 5 pages.

5. ABUSE PREVENTION AND MITIGATION:
Registry Operator should describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. A complete answer should include, but is not limited to:

- An implementation plan to establish and publish on its website a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller;
- Policies for handling complaints regarding abuse;
- Proposed measures for removal of orphan glue records for names removed from the zone when provided with evidence in written form that the glue is present in connection with malicious conduct (see Specification 6); and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

Answers must include measures to promote Whois accuracy as well as measures from one other area as described below.

- Measures to promote Whois accuracy (can be undertaken by the registry directly or by registrars via requirements in the Registry-Registrar Agreement (RRA)) may include, but are not limited to:
- Authentication of registrant information as complete and accurate at time of registration. Measures to accomplish this could include performing background checks, verifying all contact information of principals mentioned in registration data, reviewing proof of establishment documentation, and other means.
- Regular monitoring of registration data for accuracy and completeness, employing authentication methods, and establishing policies and procedures to address domain names with inaccurate or incomplete Whois data; and
- If relying on registrars to enforce measures, establishing policies and procedures to ensure compliance, which may include audits, financial incentives, penalties, or other means. Note that the requirements of the RAA will continue to apply to all ICANN-accredited registrars.
- A description of policies and procedures that define malicious or abusive behavior, capture metrics, and establish Service Level Requirements for resolution, including service levels for responding to law enforcement requests. This may include rapid takedown or suspension systems and sharing information regarding malicious or abusive behavior with industry partners;
- Adequate controls to ensure proper access to domain functions (can be undertaken by the registry directly or by registrars via requirements in the Registry-Registrar Agreement (RRA)) may include, but are not limited to:
- Requiring multi-factor authentication (i.e., strong passwords, tokens, one-time passwords) from registrants to process update, transfers, and deletion requests;
- Requiring multiple, unique points of contact to request and/or approve update, transfer, and deletion requests; and

- Requiring the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted.

A complete answer is expected to be no more than 20 pages.

6. RIGHTS PROTECTION MECHANISMS:
Registry Operator must describe how their registry will comply with policies and practices that minimize abusive registrations and other activities that affect the legal rights of others, such as the Uniform Domain Name Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) system, and Trademark Claims and Sunrise services at startup. A complete answer should include:

- A description of how the Registry Operator will implement safeguards against allowing unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies), and reduce opportunities for behaviors such as phishing or pharming. At a minimum, the Registry Operator must offer a Sunrise period and a Trademark Claims service during the required time periods, and implement decisions rendered under the URS on an ongoing basis; and
- A description of resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

Answers must also include additional measures specific to rights protection, such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants.

A complete answer is expected to be no more than 10 pages.

7. (A) SECURITY POLICY:
Provide a summary of the security policy for the proposed registry, including but not limited to:

- Indication of any independent assessment reports demonstrating security capabilities, and provisions for periodic independent assessment reports to test security capabilities;
- Description of any augmented security levels or capabilities commensurate with the nature of the applied for gTLD string, including the identification of any existing international or industry relevant security standards the Registry Operator commits to following (reference site must be provided);
- List of commitments made to registrants concerning security levels.

Answers must also include:

- Evidence of an independent assessment report demonstrating effective security controls (e.g., ISO 27001).

A summary of the above should be no more than 20 pages. Note that the complete security policy for the registry is required to be submitted in accordance with 8(b).

(b) Security Policy: Provide the complete security policy and procedures for the proposed registry, including but not limited to:

- System (data, server, application/services) and network access control, ensuring systems are maintained in a secure fashion, including details of how they are monitored, logged and backed up;

- Resources to secure integrity of updates between registry systems and nameservers, and between nameservers, if any;
- Independent assessment reports demonstrating security capabilities (submitted as attachments), if any;
- Provisioning and other measures that mitigate risks posed by denial of service attacks;
- Computer and network incident response policies, plans, and processes;
- Plans to minimize the risk of unauthorized access to its systems or tampering with registry data;
- Intrusion detection mechanisms, a threat analysis for the proposed registry, the defenses that will be deployed against those threats, and provision for periodic threat analysis updates;
- Details for auditing capability on all network access;
- Physical security approach;
- Identification of department or group responsible for the registry's security organization;
- Background checks conducted on security personnel;
- Description of the main security threats to the registry operation that have been identified; and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

8. TECHNICAL OVERVIEW OF PROPOSED REGISTRY:
Provide a technical overview of the proposed registry.

The technical plan must be adequately resourced, with appropriate expertise and allocation of costs. The Registry Operator will provide financial descriptions of resources in the next section and those resources must be reasonably related to these technical requirements. The overview should include information on the estimated scale of the registry's technical operation, for example, estimates for the number of registration transactions and DNS queries per month should be provided for the first two years of operation.

In addition, the overview should account for geographic dispersion of incoming network traffic such as DNS, Whois, and registrar transactions.

If the registry serves a highly localized registrant base, then traffic might be expected to come mainly from one area. This high-level summary should not repeat answers to questions below. Answers should include a visual diagram(s) to highlight dataflows, to provide context for the overall technical infrastructure. Detailed diagrams for subsequent questions should be able to map back to this high-level diagram(s). The visual diagram(s) can be supplemented with documentation, or a narrative, to explain how all of the Technical & Operational components conform.

A complete answer is expected to be no more than 10 pages.

9. ARCHITECTURE:
Provide documentation for the system and network architecture that will support registry operations for

the proposed scale of the registry. System and network architecture documentation must clearly demonstrate the Registry Operator's ability to operate, manage, and monitor registry systems. Documentation should include multiple diagrams or other components including but not limited to:

- Detailed network diagram(s) showing the full interplay of registry elements, including but not limited to SRS, DNS, Whois, data escrow, and registry database functions;
    - Network and associated systems necessary to support registry operations, including:
    - Anticipated TCP / IP addressing scheme,
    - Hardware (i.e., servers, routers, networking components, virtual machines and key characteristics (CPU and RAM, Disk space, internal network connectivity, and make and model)),
    - Operating system and versions, and
    - Software and applications (with version information) necessary to support registry operations, management, and monitoring
- General overview of capacity planning, including bandwidth allocation plans;
- List of providers / carriers; and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

Answers must also include evidence of a network architecture design that greatly reduces the risk profile of the proposed registry by providing a level of scalability and adaptability (e.g., protection against DDoS attacks) that far exceeds the minimum configuration necessary for the expected volume.

A complete answer is expected to be no more than 10 pages.

10. DATABASE CAPABILITIES:

Provide details of database capabilities including but not limited to:

- Database software;
- Storage capacity (both in raw terms [e.g., MB, GB] and in number of registrations/registration transactions);
- Maximum transaction throughput (in total and by type of transaction);
- Scalability;
- Procedures for object creation, editing, and deletion, and user and credential management;
- High availability;
- Change management procedures;
- Reporting capabilities; and

- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A registry database data model can be included to provide additional clarity to this response.

Note: Database capabilities described should be in reference to registry services and not necessarily related support functions such as Personnel or Accounting, unless such services are inherently intertwined with the delivery of registry services.

Answers must also include evidence of database capabilities that greatly reduce the risk profile of the proposed registry by providing a level of scalability and adaptability that far exceeds the minimum configuration necessary for the expected volume.

A complete answer is expected to be no more than 5 pages.

11. GEOGRAPHIC DIVERSITY:
Provide a description of plans for geographic diversity of:

a. Name servers, and
b. Operations centers.

Answers should include, but are not limited to:

- The intended physical locations of systems, primary and back-up operations centers (including security attributes), and other infrastructure;
- Any registry plans to use Anycast or other topological and geographical diversity measures, in which case, the configuration of the relevant service must be included;
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the
- Criteria (number and description of personnel roles allocated to this area).

Answers must also include evidence of a geographic diversity plan that greatly reduces the risk profile of the proposed registry by ensuring the continuance of all vital business functions (as identified in the Registry Operator's continuity plan in Question 17) in the event of a natural or other disaster) at the principal place of business or point of presence.

12. DNS SERVICE:
Describe the configuration and operation of nameservers, including how the Registry Operator will comply with relevant RFCs.

All name servers used for the new gTLD must be operated in compliance with the DNS protocol specifications defined in the relevant RFCs, including but not limited to: 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472.

- Provide details of the intended DNS Service including, but not limited to: A description of the DNS services to be provided, such as query rates to be supported at initial operation, and reserve capacity of the system. Describe how your nameserver update methods will change at various scales. Describe how DNS performance will change at various scales.
- RFCs that will be followed – describe how services are compliant with RFCs and if these are dedicated or shared with any other functions (capacity/performance) or DNS zones.
- The resources used to implement the services - describe complete server hardware and software, including network bandwidth and addressing plans for servers. Also include resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).
- Demonstrate how the system will function - describe how the proposed infrastructure will be able to deliver the performance described in Specification 10 (section 2) attached to the Registry Agreement.

Examples of evidence include:

- Server configuration standard (i.e., planned configuration).
- Network addressing and bandwidth for query load and update propagation.
- Headroom to meet surges.

A complete answer is expected to be no more than 10 pages.

13. IPV6 REACHABILITY:
Provide a description of plans for providing IPv6 transport including, but not limited to:

- How the registry will support IPv6 access to Whois, Web-based Whois and any other Registration Data Publication Service as described in Specification 6 (section 1.5) to the Registry Agreement.
- How the registry will comply with the requirement in Specification 6 for having at least two nameservers reachable over IPv6.
- List all services that will be provided over IPv6, and describe the IPv6 connectivity and provider diversity that will be used.
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages.

14. DATA BACKUP POLICIES & PROCEDURES:
Provide:

- Details of frequency and procedures for backup of data,
- Hardware, and systems used for backup,
- Data format,

- Data backup features,
- Backup testing procedures,
- Procedures for retrieval of data/rebuild of database,
- Storage controls and procedures, and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages.

15. DATA ESCROW:
Describe:

- How the Registry Operator will comply with the data escrow requirements documented in the Registry Data Escrow Specification (Specification 2 of the Registry Agreement); and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages.

16. REGISTRY CONTINUITY:
Describe how the Registry Operator will comply with registry continuity 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.

Describe resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

The response should include, but is not limited to, the following elements of the business continuity plan:

- Identification of risks and threats to compliance with registry continuity obligations;
- Identification and definitions of vital business functions (which may include registry services beyond the five critical registry functions) versus other registry functions and supporting operations and
- Technology;
- Definitions of Recovery Point Objectives and Recovery Time Objective; and
- Description of testing plans to promote compliance with relevant obligations.

Answers must also include:

- A highly detailed plan that provides for leading practice levels of availability; and
- Evidence of concrete steps such as a contract with a backup provider (in addition to any currently designated service operator) or a maintained hot site.

A complete answer is expected to be no more than 15 pages.

17. REGISTRY TRANSITION:
Provide a Service Migration plan (as described in the Registry Transition Processes) that could be followed in the event that it becomes necessary to permanently transition the proposed gTLD to a new operator.
The plan must take into account, and be consistent with the vital business functions identified in the previous question.

Elements of the plan may include, but are not limited to:

- Preparatory steps needed for the transition of critical registry functions;
- Monitoring during registry transition and efforts to minimize any interruption to critical registry functions during this time; and
- Contingency plans in the event that any part of the registry transition is unable to move forward according to the plan.

A complete answer is expected to be no more than 10 pages.

18. FAILOVER TESTING:
Provide:

- A description of the failover testing plan, including mandatory annual testing of the plan. Examples may include a description of plans to test failover of data centers or operations to alternate sites, from a hot to a cold facility, registry data escrow testing, or other mechanisms. The plan must take into account and be consistent with the vital business functions identified in Question 17; and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

The failover testing plan should include, but is not limited to, the following elements:

- Types of testing (e.g., walkthroughs, takedown of sites) and the frequency of testing;
- How results are captured, what is done with the results, and with whom results are shared;
- How test plans are updated (e.g., what triggers an update, change management processes for making updates);
- Length of time to restore critical registry functions;
- Length of time to restore all operations, inclusive of critical registry functions; and
- Length of time to migrate from one site to another.

A complete answer is expected to be no more than 10 pages.

19. MONITORING AND FAULT ESCALATION PROCESSES:
Provide:

- A description of the proposed (or actual) arrangements for monitoring critical registry systems (including SRS, database systems, DNS servers, Whois service, 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.
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

Answers must also include:

- Meeting the fault tolerance/monitoring guidelines described
- Evidence of commitment to provide a 24x7 fault response team.

A complete answer is expected to be no more than 10 pages.

20. DNSSEC:
Provide:

- The registry's DNSSEC policy statement (DPS), which should include the policies and procedures the proposed registry will follow, for example, for signing the zone file, for verifying and accepting DS records from child domains, and for generating, exchanging, and storing keying material;
- Describe how the DNSSEC implementation will comply with relevant RFCs, including but not limited to: RFCs 4033, 4034, 4035, 5910, 4509, 4641, and 5155 (the latter will only be required if Hashed Authenticated Denial of Existence will be offered); and
- Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 5 pages. Note, the DPS is required to be submitted as part of the application.

21. THIS QUESTION IS OPTIONAL BUT MUST BE ANSWERED IF THE REGISTRY CURRENTLY OFFERS IDNs.
IDNs:

- State whether the proposed registry will support the registration of IDN labels in the TLD, and if so, how. For example, explain which characters will be supported, and provide the associated IDN Tables with variant characters identified, along with a corresponding registration policy. This includes public interfaces to the databases such as Whois and EPP.
- Describe how the IDN implementation will comply with RFCs 5809-5893 as well as the ICANN IDN Guidelines at: http://www.icann.org/en/topics/idn/implementation-guidelines.htm.
- Describe resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer is expected to be no more than 10 pages plus attachments.