Draft Applicant Guidebook, v4

Module 5

Please note that this is a discussion draft only. Potential applicants should not rely on any of the proposed details of the new gTLD program as the program remains subject to further consultation and revision.

31 May 2010

Module 5

Transition to Delegation

This module describes the final steps required of an applicant for completion of the process, including execution of a registry agreement with ICANN and preparing for delegation of the new gTLD into the root zone.

5.1 Registry Agreement

All applicants that have successfully completed the evaluation process—including, if necessary, the dispute resolution and string contention processes—are required to enter into a registry agreement with ICANN before~~in order to~~ proceeding to delegation.

The draft registry agreement can be reviewed in the attachment to this module. All successful applicants are expected to enter into the agreement substantially as written. It is important to note that the agreement referred to above does not constitute a formal position by ICANN and has not been approved by the ICANN Board of Directors. The agreement is set out in draft form for review and community discussion purposes and as a means to improve the effectiveness of the agreement in providing for increased competition and choice for consumers in a stable, secure DNS.

Prior to entry into a registry agreement with an applicant, ICANN may conduct a pre-contract review. To ensure that an applicant continues to be a going concern in good legal standing, ICANN reserves the right to ask the applicant to submit updated documentation and information before entering into the registry agreement. Entry into any registry agreement by ICANN must first be approved by the ICANN Board of Directors.

Prior to or concurrent with the execution of the registry agreement, the applicant must also provide documentary evidence of its ability to fund ~~ongoing basic~~ critical registry functions~~operations~~ for its future registrants for a period of three~~ to five~~ years in the event of registry failure, default or until a successor operator can be designated. This obligation is met by securing a financial instrument

("continued operations instrument") as described in the Evaluation Criteria.

5.2 Pre-Delegation Testing

Each applicant will be required to complete pre-delegation technical testing as a prerequisite to delegation into the root zone. This pre-delegation test must be completed within the time period specified in the registry agreement.

The purpose of the pre-delegation technical test is to verify the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described in Module 2.

The test is intended to indicate that the applicant can operate the gTLD in a stable and secure manner. All applicants will be tested on a pass/fail basis according to the requirements that follow.

The test elements cover both the DNS server operational infrastructure and registry system operations. In many cases the applicant will perform the test elements as instructed and provide documentation of the results to ICANN to demonstrate satisfactory performance. At ICANN's discretion, aspects of the applicant's self-certification documentation can be audited either on-site at the services delivery point of the registry or elsewhere as determined by ICANN.

5.2.1 Testing Procedures

The applicant may initiate the pre-delegation test by submitting to ICANN the Pre-Delegation form and accompanying documents containing all of the following information:

- All name server names and IPv4/IPv6 addresses to be used in serving the new TLD data;
- If using anycast, the list of names and IPv4/IPv6 unicast addresses allowing the identification of each individual server in the anycast sets;
- If IDN is supported, the complete IDN tables used in the registry system;

- The new TLD zone must be signed at test time and the valid key-set to be used at the time of testing must be provided to ICANN in the documentation, as well as the TLD DNSSEC Policy Statement (DPS);

- The ~~Its~~ executed agreement between the ~~with its~~ selected escrow agent~~;~~ and the applicant;

- Self-certification documentation as described below for each test item.

ICANN will review the material submitted and in some cases perform additional tests. After ~~these cycles of~~ testing, ICANN will assemble a report with the outcome of the tests and provide that report to~~communicate with~~ the applicant.

Any clarification request, additional information request, or ~~general ICANN~~ other request generated in the process will be highlighted and listed in the report sent to the applicant.

ICANN may request the applicant to complete load tests considering an aggregated load where a single entity is performing registry services for multiple TLDs.

Once an applicant has met all of the pre-delegation testing requirements, it is eligible to request delegation of its applied-for gTLD. ~~All delegations to the root zone must also be approved by the ICANN Board of Directors.~~

If an applicant does not complete the pre-delegation steps within the time period specified in the registry agreement, ICANN reserves the right to terminate the registry agreement.

5.2.2 Test Elements: DNS Infrastructure

The first set of test elements concerns the DNS infrastructure of the new gTLD ~~and is described here~~. In all tests of the DNS infrastructure, all requirements are independent of whether IPv4 or IPv6 is used. All tests shall be done both over IPv4 and IPv6, with reports providing results according to both protocols.[1]

[1] IPv6 capabilities are embedded into multiple testing areas; this is a change from previous versions where IPv6 was specified as an individual test element.

~~System performance requirements~~UDP Support **--** The DNS infrastructure to which these tests apply comprises the complete set of servers and network infrastructure to be used by the chosen providers to deliver DNS service for the new gTLD to the Internet. The documentation provided by the applicant must include the results from a system performance test indicating available network and server capacity ~~available~~ and an estimate of expected capacity during normal operation to ensure stable service as well as to adequately address Distributed Denial of Service (DDoS) attacks.

Self-certification documentation shall include data on load capacity, latency and network reachability.

Load capacity shall be reported using a table, and a corresponding graph, showing percentage of queries responded against an increasing number of queries per second generated from local~~,~~ (to the servers)~~,~~ traffic generators. The table shall include at least 20 data points and loads of UDP-based queries that will cause up to ~~a~~ 10% query loss against a randomly selected subset of servers within the applicant's DNS infrastructure. Responses must either contain zone data or be NXDOMAIN or NODATA responses to be considered valid.

Query ~~l~~latency shall~~will~~ be reported in milliseconds as measured by DNS probes located just outside the border routers of the physical network hosting the name servers, from a network topology point of view.

Reachability will be documented by providing information on the transit and peering arrangements for the DNS server locations, listing the AS numbers of the transit providers or peers at each point of presence and available bandwidth at those points of presence.

TCP support -- TCP transport service for DNS queries and responses must be enabled and provisioned for expected load. ICANN will review the capacity self-certification documentation provided by the applicant and will perform TCP reachability and transaction capability tests across a randomly selected subset of the ~~for each applicant listed~~ name servers within the applicant's DNS infrastructure. In case of use of anycast, each individual server in each anycast set will be tested.

Self-certification documentation shall include data on load capacity, latency and external network reachability.

Load capacity shall be reported using a table, and a corresponding graph, showing percentage of queries that generated a valid (zone data, NODATA, or NXDOMAIN) response ~~responded~~ against an increasing number of queries per second generated from local ~~,~~ (to the name servers)~~,~~ traffic generators. The table shall include at least 20 data points and loads that will cause up to ~~a~~ 10% query loss (either due to connection timeout or connection reset) against a randomly selected subset of servers within the applicant's DNS infrastructure. ~~Responses must either contain zone data or be NXDOMAIN or NODATA responses to be considered valid.~~

Query l~~L~~atency will be reported in milliseconds as measured by DNS probes located just outside the border routers of the physical network hosting the name servers, from a network topology point of view.

Reachability will be documented by providing records of TCP-~~-~~based DNS queries from nodes external to the network hosting the servers. These locations may be the same as those used for measuring latency above.

~~***IPv6 support*** -- Applicant must provision IPv6 service for its DNS infrastructure. ICANN will review the self-certification documentation provided by the applicant and will test IPv6 reachability from various points on the Internet. DNS transaction capacity over IPv6 for all name servers with declared IPv6 addresses will also be checked. In case of use of anycast, each individual server in each anycast set will be tested.~~

~~Self-certification documentation shall include data on load capacity, latency and external network reachability.~~

~~For the set of DNS servers that support IPv6, load capacity shall be reported using a table, and a corresponding graph, showing percentage of queries responded against an increasing number of queries per second generated from local, to the servers, traffic generators. The table shall include at least 20 data points and loads that will cause up to a 10% query loss. Responses must either contain zone data or be NXDOMAIN or NODATA responses to be considered valid.~~

~~Latency will be reported in milliseconds as measured by DNS probes located just outside the border routers of the physical network hosting the servers.~~

~~Reachability will be documented by providing records of DNS queries over IPv6 transport from nodes external to the network hosting the servers. In addition, applicant shall provide details of its IPv6 transit and peering arrangements, including a list of AS numbers with which it exchanges IPv6 traffic.~~

DNSSEC support -- Applicant must demonstrate support for EDNS(0) in its server infrastructure, the ability to return correct DNSSEC-related resource records such as DNSKEY, RRSIG, and NSEC/NSEC3 for the signed zone, and the ability to accept and publish DS resource records from second-level domain administrators. In particular, the applicant must demonstrate its ability to support the full life cycle of KSK and ZSK keys. ICANN will review the self-certification materials as well as test the reachability, response sizes, and DNS transaction capacity for DNS queries using the EDNS(0) protocol extension with the "DNSSEC OK" bit set for ~~each~~ a randomly selected subset of all name servers within the applicant's DNS infrastructure. In case of use of anycast, each individual server in each anycast set will be tested.

Load capacity, query latency, and reachability shall be documented as for UDP and TCP above.

5.2.3 Test Elements: Registry Systems

As documented in the registry agreement, registries must provide support for EPP within their Shared Registration System, and provide Whois service both via port 43 and a web interface, in addition to support for the DNS ~~infrastructure~~. This section details the requirements for testing these registry systems.

System performance -- The registry system must scale to meet the performance requirements described in Specification 6 of the registry agreement and ICANN will require self-certification of compliance. ICANN will review the self-certification documentation provided by the applicant to verify adherence to these minimum requirements.

Whois support -- Applicant must provision Whois services for the anticipated load. ICANN will verify that Whois data is accessible over IPv4 and IPv6 via both TCP port 43 and via a web interface and review self-certification documentation regarding Whois transaction capacity. Response format according to Specification 4 of the registry agreement and ~~A~~access to Whois (both port 43 and via ~~the~~ web) will be tested by ICANN remotely from various points on the Internet over both IPv4 and IPv6.

Self-certification documents shall describe the maximum number of queries per second successfully handled by both the port 43 servers as well as the web interface, together with an applicant-provided load expectation.

Additionally, a description of deployed control functions to detect and mitigate data mining of the Whois database shall be documented.

EPP Support -- As part of a shared registration service, applicant must provision EPP services for the anticipated load. ICANN will verify conformance to appropriate RFCs (including EPP extensions for DNSSEC). ICANN will also review self-certification documentation regarding EPP transaction capacity.

Documentation shall provide a maximum Transaction per Second rate for the EPP interface with 10 data points corresponding to registry database sizes from 0 (empty) to the expected size after one year of operation, as determined by applicant.

Documentation shall also describe measures taken to handle load during initial registry operations, such as a land-rush period.

IPv6 support -- The ability of the registry to support registrars adding, changing, and removing IPv6 DNS records supplied by registrants will be tested by ICANN. If the registry supports EPP access via IPv6, this will be tested by ICANN remotely from various points on the Internet.

DNSSEC support -- ICANN will review the ability of the registry to support registrars adding, changing, and removing DNSSEC-related resource records as well as the registry's overall key management procedures. In particular, the applicant must demonstrate its ability to

support the full life cycle of key changes for child domains. Inter-operation of the applicant's secure communication channels with the IANA for trust anchor material exchange will be verified.

The practice and policy document (also known as the DNSSEC Policy Statement or DPS), describing key material storage, access and usage for its own keys and the registrants' trust anchor material, is also reviewed as part of this step.

IDN support -- ICANN will verify the complete IDN table(s) used in the registry system. The table(s) must comply with the guidelines in http://iana.org/procedures/idn-repository.html.

Requirements related to IDN for Whois are being developed. After these requirements are developed, prospective registries will be expected to comply with published IDN-related Whois requirements as part of pre-delegation testing.

Escrow deposit -- The applicant-provided samples of ~~dummy~~ data deposit that include~~,~~ both a~~one~~ full and ~~one~~ an incremental deposit~~,~~ showing correct type and formatting of content will be reviewed. Special attention will be given to the agreement with the ~~applicant~~ escrow provider to ensure that escrowed data can be released within 24 hours in case of emergency ~~recovered~~ and the registry reconstituted within one business day to the point where it can respond to DNS and Whois queries ~~(both via port 43 and via the web)~~ should it be necessary. ICANN may, at its option, ask an independent third party to demonstrate the reconstitutability of the registry from escrowed data.

5.3 Delegation Process

Upon notice of successful completion of the ICANN pre-delegation testing, applicants may initiate the process for delegation of the new gTLD into the root zone database. This will include provision of additional information and completion of additional technical steps required for delegation. ~~-~~Information about the delegation process is available at http://iana.org/domains/root/.

5.4 Ongoing Operations

An applicant that is successfully delegated a gTLD will become a "Registry Operator." In being delegated the role of operating part of the Internet's domain name system, the applicant will be assuming a number of significant responsibilities. ICANN will hold all new gTLD operators accountable for the performance of their obligations under the registry agreement, and it is important that all applicants understand these responsibilities.

5.4.1 What is Expected of a Registry Operator

The registry agreement defines the obligations of gTLD registry operators. A breach of the registry operator's obligations may result in ICANN compliance actions up to and including termination of the registry agreement. Prospective applicants are encouraged to review the following brief description of some of these responsibilities.

Note that this is a non-exhaustive list provided to potential applicants as an introduction to the responsibilities of a registry operator. For the complete and authoritative text, please refer to the draft registry agreement.

A registry operator is obligated to:

Operate the TLD in a stable and secure manner. The registry operator is responsible for the entire technical operation of the TLD. As noted in RFC 1591:

"The designated manager must do a satisfactory job of operating the DNS service for the domain. That is, the actual management of the assigning of domain names, delegating subdomains and operating nameservers must be done with technical competence. This includes keeping the central IR[2] (in the case of top-level domains) or other higher-level domain manager advised of the status of the domain, responding to requests in a timely manner, and operating the database with accuracy, robustness, and resilience."

The registry operator is required to comply with relevant technical standards in the form of RFCs and other guidelines. Additionally, the registry operator must meet

[2] IR is a historical reference to "Internet Registry," a function now performed by ICANN.

performance specifications in areas such as system downtime and system response times (see Specification 6 of the draft Registry Agreement).

Comply with consensus policies and temporary policies. gTLD registry operators are required to comply with consensus policies. Consensus policies may relate to a range of topics such as issues affecting interoperability of the DNS, registry functional and performance specifications, database security and stability, or resolution of disputes over registration of domain names.

To be adopted as a consensus policy, a policy must be developed by the Generic Names Supporting Organization (GNSO)[3] following the process in Annex A of the ICANN Bylaws.[4] The policy development process involves deliberation and collaboration by the various stakeholder groups~~constituencies~~ participating in the process, with multiple opportunities for input and comment by the public, and can take significant time.

Examples of existing consensus policies are the Inter-Registrar Transfer Policy (governing transfers of domain names between registrars), and the Registry Services Evaluation Policy (establishing a review of proposed new registry services for security and stability or competition concerns), although there are several more, as found at http://www.icann.org/en/general/consensus-policies.htm.

gTLD registry operators are obligated to comply with both existing consensus policies and those that are developed in the future. Once a consensus policy has been formally adopted, ICANN will provide gTLD registry operators with notice of the requirement to implement the new policy and the effective date.

In addition, the ICANN Board may, when required by circumstances, establish a temporary policy necessary to maintain the stability or security of registry services or the DNS. In such a case, all gTLD registry operators will be required to comply with the temporary policy for the designated period of time.

For more information, see Specification 1 of the draft Registry Agreement.

[3] http://gnso.icann.org
[4] http://www.icann.org/en/general/bylaws.htm#AnnexA

Implement start-up rights protection measures. The registry operator must implement, at a minimum, either a Sunrise period or a Trademark Claims service during the start-up phases for registration in the TLD. These mechanisms will be supported by the established Trademark Clearinghouse as indicated by ICANN. The Sunrise period allows eligible rightsholders an early opportunity to register names in the TLD. The Trademark Claims service provides notice to potential registrants of existing trademark rights, as well as notice to rightsholders of relevant names registered. Registry operators may continue offering the Trademark Claims service after the relevant start-up phases have concluded. For more information, see Specification 7 of the draft Registry Agreement and the Trademark Clearinghouse model accompanying this module.

Implement post-launch rights protection measures. The registry operator is required to implement decisions made under the Uniform Rapid Suspension (URS) procedure, including suspension of specific domain names within the registry. The registry operator is also required to comply with and implement decisions made according to the Trademark Post-Delegation Dispute Resolution Policy (PDDRP). ~~In addition, the registry operator must comply with the specific rights protection mechanisms developed and included in the registry agreement (See Specification 7 to the draft agreement).~~ The required measures are described fully in the URS and PDDRP procedures accompanying this module. Registry operators may introduce additional rights protection measures relevant to the particular gTLD.

Implement measures for protection of country and territory~~geographical~~ names in the new gTLD. All new gTLD registry operators are required to provide certain minimum protections for country and territory names, including an initial reservation requirement and establishment of~~any~~ applicable rules and procedures for release of these names. Registry operators are encouraged to implement measures for protection of geographical names in addition to those required by the agreement, according to the needs and interests of each gTLD's particular circumstances. (See Specification 5 of the draft registry agreement).

Pay recurring fees to ICANN. In addition to existing expenditures made to accomplish the objectives set out in ICANN's mission statement, these funds enable the support

required for new gTLDs, including: contractual compliance, registry liaison, increased registrar accreditations, and other registry support activities. The fees include both a fixed component (USD 25,000 annually) and, once the TLD has passed a threshold size, a variable fee based on transaction volume. See Article 6 of the draft registry agreement.

Regularly deposit data into escrow. This serves an important role in registrant protection and continuity for certain instances where the registry or one aspect of the registry operations experiences a system failure or loss of data. (See Specification 2 of the draft registry agreement.)

Deliver monthly reports in a timely manner. A registry operator must submit a report to ICANN on a monthly basis. The report includes performance statistics for the month, registrar transactions, and other data, and is used by ICANN for compliance purposes as well as calculation of registrar fees. (See Specification 3 of the draft registry agreement.)

Provide Whois service. A registry operator must provide a publicly available Whois service for registered domain names in the TLD. (See Specification 4 of the draft registry agreement.)

Maintain partnerships with ICANN-accredited registrars. A registry operator creates a Registry-Registrar Agreement (RRA) to define requirements for its registrars. This must include certain terms that are specified in the Registry Agreement, and may include additional terms specific to the TLD. A registry operator must provide non-discriminatory access to its registry services to all ICANN-accredited registrars with whom it has entered into an RRA, and who are in compliance with the requirements. This includes providing advance notice of pricing changes to all registrars, in compliance with the time frames specified in the agreement. (See Article 2 of the draft registry agreement.)

Maintain an abuse point of contact. A registry operator must maintain and publish on its website a single 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. (See Specification 6 of the draft registry agreement.)

Cooperate with contractual compliance audits. To maintain a level playing field and a consistent operating environment, ICANN staff performs periodic audits to assess contractual compliance and address any resulting problems. A registry operator must provide documents and information requested by ICANN that are necessary to perform such audits. (See Article 2 of the draft registry agreement.)

Maintain a Continued Operations Instrument. A registry operator must, at the time of the agreement, have in place a continued operations instrument sufficient to fund basic registry operations for a period of three (3) years. This requirement remains in place for five (5) years after delegation of the TLD, after which time the registry operator is no longer required to maintain the continued operations instrument. (See Specification 8 to the draft registry agreement.)

Maintain community-based policies and procedures. If the registry operator designated its application as community-based at the time of the application, the registry operator has requirements in its registry agreement to maintain the community-based policies and procedures it specified in its application. The registry operator is bound by the Registry Restrictions Dispute Resolution Procedure with respect to disputes regarding execution of its community-based policies and procedures. (See Article 2 to the draft registry agreement.)

Have continuity and transition plans in place. This includes designation of a transition provider, as well as performing failover testing on a regular basis. In the event that a transition to a new registry operator becomes necessary, the registry operator is expected to cooperate by consulting with ICANN on the appropriate successor, providing the data required to enable a smooth transition, and complying with the applicable registry transition procedures. (See the "Registry Transition Processes" explanatory memo for a discussion of transition procedures.)

Make TLD zone files available via a standardized process. This includes provision of access to the registry's zone file to credentialed users, according to established access, file, and format standards. The registry operator will enter into a

standardized form of agreement with zone file users and will accept credential information for users via a clearinghouse. For more information, see Specification 4 of the draft Registry Agreement and the "Zone File Access for the Future" strategy proposal.

Implement DNSSEC. The registry operator is required to sign the TLD zone files implementing Domain Name System Security Extensions (DNSSEC) in accordance with the relevant technical standards. The registry must accept public key material from registrars for domain names registered in the TLD, and publish a DNSSEC Policy Statement describing key material storage, access, and usage for the registry's keys and the registrants' trust anchor material. For more information, see Specification 6 of the draft Registry Agreement.

5.4.2 What is Expected of ICANN

ICANN will continue to provide support for gTLD registry operators as they launch and maintain registry operations. ICANN's gTLD registry liaison function provides a point of contact for gTLD registry operators for assistance on a continuing basis.

ICANN's contractual compliance function will ~~also~~ perform audits on a regular basis to ensure that gTLD registry operators remain in compliance with agreement obligations, as well as investigate any complaints from the community regarding the registry operator's adherence to its contractual obligations. See http://www.icann.org/en/compliance/ for more information on current contractual compliance activities.

ICANN's Bylaws require ICANN to act in an open and transparent manner, and to provide equitable treatment among registry operators. ICANN is responsible for maintaining the security and stability of the global Internet, and looks forward to a constructive and cooperative relationship with future gTLD registry operators in furtherance of this goal.