



Draft Applicant Guidebook, v2

Module 2

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.

18 February 2009

Module 2

Evaluation Procedures

This module describes the evaluation procedures and criteria used to determine whether applied-for gTLDs are approved for delegation. All applicants will undergo an Initial Evaluation and those that do not pass all elements may request Extended Evaluation.

The first, required evaluation is the **Initial Evaluation**, during which ICANN first assesses an applied-for gTLD string, an applicant's qualifications, and its proposed registry services.

The following elements make up **Initial Evaluation**:

- String Reviews
 - String confusion
 - Reserved names
 - DNS stability
 - Geographical names
- Applicant Reviews
 - Demonstration of technical and operational capability
 - Demonstration of financial capability
 - Registry services

An applicant must pass all these reviews to pass the Initial Evaluation. Failure to pass any one of these reviews will result in a failure to pass the Initial Evaluation.

Extended Evaluation may be applicable in cases in which an applicant does not pass the Initial Evaluation. See Section 2.2 below.

2.1 Initial Evaluation

The Initial Evaluation consists of two types of review. Each type is composed of several elements.

The first review focuses on the applied-for gTLD string to test:

- Whether the applied-for gTLD string is so similar to others that it would cause user confusion;
- Whether the applied-for gTLD string might adversely affect DNS security or stability; and
- Whether requisite government approval is given in the case of certain geographical names.

The second review focuses on the applicant to test:

- Whether the applicant has the requisite technical, operational, and financial capability; and
- Whether the registry services offered by the applicant might adversely affect DNS security or stability.

2.1.1 String Reviews

In the Initial Evaluation, ICANN reviews every applied-for gTLD string. Those reviews are described in greater detail in the following subsections.

2.1.1.1 String Confusion Review

The objective of this review is to prevent user confusion and loss of confidence in the DNS. This review involves a preliminary comparison of each applied-for gTLD string against existing TLDs and against other applied-for gTLD strings. The review is to determine whether the applied-for gTLD string is so similar to one of the others that it would create a probability of detrimental user confusion if it were to be delegated to the root zone. The visual similarity check that occurs during Initial Evaluation is intended to augment the objection and dispute resolution process (see Module 3, Dispute Resolution Procedures) that addresses all types of similarity.

This similarity review will be conducted by a panel of String Similarity Examiners. It will be informed in part by an algorithmic score for the visual similarity between each applied-for string and each of other existing and applied-for TLDs. The score will provide one objective measure for consideration by the panel.

The examiners' task is to identify visual string similarities that would create a probability of detrimental user confusion. The examiners will use a common standard to test for whether string confusion exists, as follows:

Standard for String Confusion – String confusion exists where a string so nearly resembles another visually that it is likely to

deceive or cause confusion. For the likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion.

The standard will be applied in three sets of circumstances, when comparing:

- Applied-for gTLD strings against existing TLDs and reserved names;
- Applied-for gTLD strings against other applied-for gTLD strings; and
- Applied-for gTLD strings against strings requested as IDN ccTLDs.

Similarity to Existing TLDs – This review involves cross-checking between each applied-for string and the list of existing TLD strings to determine whether the two strings are so similar to one another that they create a probability of detrimental user confusion.

All TLDs currently in the root zone can be found at <http://iana.org/domains/root/db/>.

An application that fails the string confusion review and is found too similar to an existing TLD will not pass the Initial Evaluation, and no further reviews will be available.

In the simple case in which an applied-for TLD string is identical to an existing TLD, the application system will recognize the existing TLD and will not allow the application to be submitted.

Testing for identical strings also takes into consideration the code point variants listed in any relevant language reference table. For example, protocols treat equivalent labels as alternative forms of the same label, just as “foo” and “Foo” are treated as alternative forms of the same label (RFC 3490).

An application that passes this preliminary string confusion review is still subject to challenge by an existing TLD operator or by another gTLD applicant in the current application round. That process requires that a specific objection be filed by an objector having the standing to make such an objection. Such category of objection is not limited to visual similarity. Rather, confusion based on any type of similarity (including visual, aural, or similarity of

meaning) may be claimed by an objector. Refer to Module 3, Dispute Resolution Procedures, for more information about the objection process.

Similarity to Other Applied-for gTLD Strings (String Contention Sets) – All applied-for gTLD strings will be reviewed against one another to identify any strings that are so similar that they create a probability of detrimental user confusion if more than one is delegated into the root zone. In performing the string confusion review, the panel of String Similarity Examiners will create contention sets that may be used in later stages. A contention set contains at least two applied-for strings identical to one another or so similar that string confusion would result if more than one were delegated into the root zone. Refer to Module 4, String Contention Procedures, for more information on contention sets and contention resolution. ICANN will notify applicants who are part of a contention set by the conclusion of the Initial Evaluation period. These contention sets will also be published on ICANN’s website.

An applicant may file a formal objection against another gTLD application on string confusion grounds (see Module 3, Dispute Resolution Procedures). Such an objection may, if successful, change the configuration of the previously-configured contention sets in that the two applied-for gTLD strings will be considered in direct contention with one another (see Module 4, String Contention Procedures). The objection process will not result in removal of an application from a contention set.

Similarity to TLD strings requested as IDN ccTLDs -- Applied-for gTLD strings will also be reviewed for similarity to TLD strings requested in the IDN ccTLD Fast Track process (see <http://www.icann.org/en/topics/idn/fast-track/>). Should conflict with a prospective fast-track IDN ccTLD be identified, ICANN will take the following approach to resolving the conflict.

If one of the applications has completed its respective process before the other is lodged, that TLD will be delegated. A gTLD application that has been approved by the Board will be considered complete, and therefore would not be disqualified based on contention with a newly-filed IDN ccTLD request. Similarly, an IDN ccTLD request that has completed evaluation (i.e., is “validated”) will be considered complete and therefore would not be disqualified based on contention with a newly-filed gTLD application.

If the gTLD applicant does not have the required approval from the relevant government or public authority, a validated request for an IDN ccTLD will prevail and the gTLD application will not be approved.

If both the gTLD applicant and the IDN ccTLD requestor have the required approval from the relevant government or public authority, both applications will be kept on hold until the contention is resolved through agreement between the parties, i.e., resolved by the government.

String Similarity Algorithm – The String Similarity Algorithm (“Algorithm”) is a tool the examiners use to provide one objective measure as part of the process of identifying strings likely to result in confusion. The Algorithm will be available in multiple scripts. The Algorithm is also available to applicants for testing and informational purposes. The Algorithm, user guidelines, and additional background information are available at <http://icann.sword-group.com/icann-algorithm/>.

The Algorithm calculates scores for visual similarity between any two strings, using factors such as letters in sequence, number of similar letters, number of dissimilar letters, common prefixes, common suffixes, hyphenation, and string length¹. Note that hyphens are ignored when performing the comparison, so the string “E-X-A-M-P-L-E” would be scored by the Algorithm as identical to the string “EXAMPLE.”

2.1.1.2 *Reserved Names Review*

The Reserved Names review involves comparison with the list of top-level Reserved Names to ensure that the applied-for gTLD string does not appear on that list.²

¹ ICANN received some questions concerning the Algorithm’s incorporation of factors such as keyboard proximity, to guard against typosquatting. Keyboard proximity is not addressed as a special category of similarity, as gTLDs are used globally, and keyboards vary from one country to another. However, the purpose of the string similarity check is to avoid confusion and it is expected that typosquatting attempts by applicants will be recognized by the Algorithm or by the Examiners.

² The Top-Level Reserved Names List has not changed for this draft of the guidebook. Some comments questioned the inclusion of ICANN’s name and the names of ICANN structures on the list. ICANN has taken a conservative approach by including names already reserved at the second level in most gTLDs, and will undertake the work recommended by the GNSO’s Reserved Names Working Group in regard to treatment of the ICANN names. Additionally, comments suggested addition of other categories of names, such as well-known brands or geographical names to the Top-Level Reserved Names List. Discussion of these issues is included in the Public Comment Analysis at <http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf>.

Top-Level Reserved Names List

| | | |
|---------------------|---------------------|---------------------|
| <i>AFRINIC</i> | <i>IANA-SERVERS</i> | <i>NRO</i> |
| <i>ALAC</i> | <i>ICANN</i> | <i>RFC-EDITOR</i> |
| <i>APNIC</i> | <i>IESG</i> | <i>RIPE</i> |
| <i>ARIN</i> | <i>IETF</i> | <i>ROOT-SERVERS</i> |
| <i>ASO</i> | <i>INTERNIC</i> | <i>RSSAC</i> |
| <i>CCNSO</i> | <i>INVALID</i> | <i>SSAC</i> |
| <i>EXAMPLE*</i> | <i>IRTF</i> | <i>TEST*</i> |
| <i>GAC</i> | <i>ISTF</i> | <i>TLD</i> |
| <i>GNSO</i> | <i>LACNIC</i> | <i>WHOIS</i> |
| <i>GTLD-SERVERS</i> | <i>LOCAL</i> | <i>WWW</i> |
| <i>IAB</i> | <i>LOCALHOST</i> | |
| <i>IANA</i> | <i>NIC</i> | |

*Note that in addition to the above strings, ICANN will reserve translations of the terms "test" and "example" in multiple languages. The remainder of the strings are reserved only in the form included above.

If an applicant enters a Reserved Name as its applied-for gTLD string, the application system will recognize the Reserved Name and will not allow the application to be submitted.

In addition, applied-for gTLD strings are reviewed in a process identical to that described in the preceding section to determine whether they are similar to a Reserved Name. An application for a gTLD string that is identified as too similar to a Reserved Name will not pass the Reserved Names review.

2.1.1.3 DNS Stability Review

This review determines whether an applied-for gTLD string might cause instability to the DNS. In all cases, this will involve a review for conformance with technical and other requirements for gTLD labels. In some exceptional cases, an extended review may be necessary to investigate possible technical stability problems with the applied-for gTLD string.

2.1.1.3.1 DNS Stability: String Review Procedure

New gTLD labels must not adversely affect the security or stability of the DNS. During the Initial Evaluation period, ICANN will conduct a preliminary review on the set of applied-for gTLD strings to

- ensure that applied-for gTLD strings comply with the requirements provided in section 2.1.1.3.2 and

- determine whether any strings raise significant security or stability issues that may require further review.

There is a very low probability that an extended review will be necessary for a string that fully complies with the string requirements in subsection 2.1.1.3.2 of this module. However, the string review process provides an additional safeguard if unanticipated security or stability issues arise concerning an applied-for gTLD string.

ICANN will notify applicants who have not passed the Initial Evaluation due to security or stability concerns about the applied-for gTLD string at the conclusion of the Initial Evaluation period. Applicants will have 15 calendar days to decide whether to proceed with Extended Evaluation. See Section 2.2 for further information on the Extended Evaluation process.

2.1.1.3.2 String Requirements

ICANN will review each applied-for gTLD string to ensure that it complies with the requirements outlined in the following paragraphs.

If an applied-for gTLD string is found to violate any of these rules, the application will be denied. No further reviews are available.

Technical Requirements for all Labels (Strings) – The technical requirements for the selection of top-level domain labels follow.

- The ASCII label (i.e., the label as transmitted on the wire) must be valid as specified in the technical standards *Domain Names: Implementation and Specification* (RFC 1035), and *Clarifications to the DNS Specification* (RFC 2181). This includes the following:
 - The label must have no more than 63 characters. In the case of Punycode (IDNA2008 A-label) representations of IDN labels (U-labels), this includes the four initial characters (xn--).
 - Upper and lower case characters are considered to be syntactically and semantically identical.
- The ASCII label must be a valid host name, as specified in the technical standards *DOD Internet Host Table Specification* (RFC 952), *Requirements for*

Internet Hosts — Application and Support (RFC 1123), and *Application Techniques for Checking and Transformation of Names (RFC 3696)*. This includes the following:

- The label must consist entirely of letters, digits and hyphens.
- The label must not start or end with a hyphen.
- There must be no possibility for confusing an ASCII label for an IP address or other numerical identifier by application software. For example, representations such as "255", "o377" (255 in octal) or "0xff" (255 in hexadecimal) as the top-level domain can be interpreted as IP addresses.³. Therefore an ASCII label must not be:
 - A decimal number consisting entirely of the digits "0" through "9";
 - A hexadecimal number consisting of the digit "0" followed by the uppercase or lowercase letter "x" | "X" followed by a sequence of one or more characters all of which belong to the set of uppercase or lowercase letters "a" | "A" through "f" | "F" and the digits "0" through "9"; or
 - An octal number consisting of the uppercase or lowercase letter "o" | "O" followed by a sequence of one or more characters all of which belong to the set of digits "0" through "7."
- The ASCII label may only include hyphens in the third and fourth position if it represents a valid Internationalized Domain Name in its A-label form (ASCII encoding).
- The presentation format of the domain (i.e., either the label for ASCII domains, or the U-label for Internationalized Domain Names) must not begin or end with a digit.

Requirements for Internationalized Domain Names – These requirements apply only to prospective top-level domains

³ Refer to <http://www.icann.org/en/topics/new-gtlds/update-dns-stability-18feb09-en.pdf> for further background on octal and hexadecimal representations, and on the changes in this section.

that contain non-ASCII characters. Applicants for these internationalized top-level domain labels are expected to be familiar with the IETF IDNA standards, Unicode standards, and the terminology associated with Internationalized Domain Names.

- The label must be a valid internationalized domain name, as specified in the technical standard *Internationalizing Domain Names in Applications* (RFC 3490) or any revisions of this technical standard currently underway within the IETF. Due to this ongoing revision, the IDN-related technical requirements are subject to change. This includes, but is not limited to, the following constraints. Note that these are guidelines and are not a complete statement of the requirements of the IDNA specifications. The label:
 - Must only contain Unicode code points that are defined as “Protocol Valid” or “Contextual Rule Required” in The Unicode Codepoints and IDNA (<http://www.ietf.org/internet-drafts/draft-ietf-idnabis-tables-05.txt>), and that are accompanied, in the case of “Contextual Rule Required,” by unambiguous contextual rules.
 - Must be fully compliant with Normalization Form C, as described in *Unicode Standard Annex #15: Unicode Normalization Forms* (see examples in <http://unicode.org/faq/normalization.html>).
 - Must consist entirely of characters with the same directional property. (Note that this requirement may change with the revision of the IDNA protocol to allow for characters with no directional property defined in Unicode to be available along with either a right-to-left or a left-to-right directionality.)
- The label must meet the relevant criteria of the ICANN *Guidelines for the Implementation of Internationalised Domain Names*. See <http://www.icann.org/en/topics/idn/implementation-guidelines.htm>. This includes the following nonexhaustive list of limitations:

- o All code points in a single label must be taken from the same script as determined by the Unicode Standard Annex #24: Unicode Script Property. Exceptions are permissible for languages with established orthographies and conventions that require the commingled use of multiple scripts. However, even with this exception, visually confusable characters from different scripts will not be allowed to co-exist in a single set of permissible code points unless a corresponding policy and character table are clearly defined.

The IDNA protocol used for internationalized labels is currently under revision through the Internet standardization process. As such, additional requirements may be specified that need to be adhered to as this revision is being completed. The current status of the protocol revision is documented at <http://tools.ietf.org/wg/idnabis>.

Policy Requirements for Generic Top-Level Domains –
Applied-for strings must be composed of three or more visually distinct letters or characters in the script, as appropriate.⁴

2.1.1.4 Geographical Names

ICANN will review all applied-for gTLD strings to ensure that appropriate consideration is given to the interests of governments or public authorities in country or territory names, as well as certain other types of place names. The requirements and procedure ICANN will follow is described in the following paragraphs.

2.1.1.4.1 Categories of Strings Considered Geographical Names

The following types of applications are considered geographical names and must be accompanied by documentation of support or non-objection from the relevant government(s) or public authority(ies):

- An application for any string that is a meaningful representation of a *country or territory name* listed

⁴ ICANN received a number of comments suggesting that gTLDs consisting of fewer than three characters should be allowed in some cases, for example, in scripts featuring ideographs. The issues with defining requirements for certain cases are discussed in further detail in the Public Comment Analysis at <http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf> and ICANN invites further input on solutions.

in the ISO 3166-1 standard (see http://www.iso.org/iso/country_codes/iso_3166_data_bases.htm), as updated from time to time. A meaningful representation includes a representation of the country or territory name in any language.

A string is deemed a meaningful representation of a country or territory name if it is:

- The name of the country or territory; or
 - A part of the name of the country or territory denoting the country or territory; or
 - A short-form designation for the name of the country or territory that is recognizable and denotes the country or territory.
- An application for any string that is an exact match of a *sub-national place name*, such as a county, province, or state, listed in the ISO 3166-2 standard⁵, as updated from time to time.
 - An application for any string that is a representation, in any language, of the *capital city name* of any country or territory listed in the ISO 3166-1 standard.
 - An application for a *city name*, where the applicant declares that it intends to use the gTLD for purposes associated with the city name.
 - An application for a string which represents a *continent or UN region* appearing on the "Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings" list at <http://unstats.un.org/unsd/methods/m49/m49regin.htm>.

In the case of an application for a string which represents a continent or UN region, documentation of support, or non-objection, will be required from a substantial number of the relevant

⁵ ICANN is continuing to use the ISO 3166-1 and 2 lists as the most applicable references for the new gTLD process. The 3166-2 list is intended to be used in conjunction with the 3166-1 list, which was selected by Jon Postel as the basis for allocating ccTLDs, in the knowledge that ISO has a procedure for determining which entities should and should not be included. The ISO 3166-2 list provides an independent and dynamic source of names which is consistent with ICANN's existing processes.

governments and/or public authorities associated with the continent or the UN region.

An applied-for gTLD string that falls into any of the above categories is considered to represent a geographical name. In the event of any doubt, it is in the applicant's interest to consult with relevant governments and public authorities and enlist their support or non-objection prior to submission of the application, in order to preclude possible objections and pre-address any ambiguities concerning the string and applicable requirements.

It is the applicant's responsibility to:

- identify whether its applied-for gTLD string falls into any of the above categories; and
- determine the relevant government(s) or public authority(ies); and
- identify which level of government support is required.

The requirement to include documentation of support for certain applications does not preclude or exempt applications from being the subject of objections on community grounds (refer to subsection 3.1.1 of Module 3), under which applications may be rejected based on objections showing substantial opposition from the targeted community.

2.1.1.4.2 Documentation Requirements

The documentation of support or non-objection from the relevant government or public authority should include a signed letter of support or non-objection from the minister with the portfolio responsible for domain name administration, ICT, foreign affairs or the Office of the Prime Minister or President of the relevant jurisdiction. If there are reasons for doubt about the authenticity of the communication, ICANN will consult with the relevant diplomatic authorities or members of ICANN's Governmental Advisory Committee for the government or public authority concerned on the competent authority and appropriate point of contact within their administration for communications.

The letter must clearly express the government's or public authority's support or non-objection for the applicant's application and demonstrate the government's or public authority's understanding of the string being requested and intended use.

The letter should also demonstrate the government's or public authority's understanding that the string is being sought through the gTLD application process and the applicant is willing to accept the conditions under which the string will be available, i.e., entry into a registry agreement with ICANN requiring compliance with consensus policies and payment of fees.

2.1.1.4.3 Review Procedure for Geographical Names

A Geographic Names Panel (GNP) will be established to confirm whether each applied-for gTLD string represents a geographical name, and to verify the relevance and authenticity of the supporting documentation where necessary. It is the intention that ICANN will retain a third party to perform the function of the GNP. The Panel will examine applied-for gTLD strings against a composite database of geographic names drawn from authoritative sources, and review supporting documentation. The GNP will comprise individuals with linguistic, geographic, and governmental expertise. The Geographic Names Panel may consult with additional experts as necessary.

During the Initial Evaluation period, ICANN forwards each application to the GNP for a determination of whether the applied-for gTLD string is a geographical name (i.e., falls into any of the categories listed in subsection 2.1.1.4.1). For any applications where the applied-for gTLD string is not determined to be a geographical name, the application will pass the Geographical Names review with no additional steps required. For any application where the applied-for gTLD string is determined to be a geographical name (as described in this module), the GNP will confirm that the applicant has provided documentation from all relevant governments or public authorities, and that the communication from the government or public authority is legitimate and contains the required content.

An applicant who has not provided the required documentation will be notified of the requirement and given a limited time frame to provide it. If the time frame is not met, the application will be considered incomplete and will not pass the Initial Evaluation. The applicant may reapply in subsequent application rounds, if desired.

Note that the GNP will review all applications received, not only those where the applicant has designated its applied-for gTLD string as a geographical name.

If there is more than one application for a string representing a certain geographical name as described in

this section, and the applications are considered complete (i.e., have requisite government approvals), the applications will be suspended pending resolution by the applicants.

If an application for a string representing a geographical name is in a contention set with applications for similar strings that have not been identified as geographical names, the string contention will be settled using the string contention procedures described in Module 4.

2.1.2 Applicant Reviews

Concurrent with the applied-for gTLD string reviews described in subsection 2.1.1, ICANN will review the applicant's technical and operational capability, its financial capability, and its proposed registry services. Those reviews are described in greater detail in the following subsections.

2.1.2.1 Technical/Operational and Financial Reviews

The questions provided for applicants in the application form are available at

<http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-clean-18feb09-en.pdf>.

Applicants respond to questions which cover the following three areas in relation to themselves: general information, technical and operational capability, and financial capability.

Applicants should be aware that the application materials submitted in the online application system, as well as any evaluation materials and correspondence, will be publicly posted on ICANN's website. The sections in the application that are marked CONFIDENTIAL will not be posted. Any sections of the application that ICANN has not designated CONFIDENTIAL will be posted.

The applicant questions cover the following three areas:

General Information – These questions are intended to gather information about an applicant's legal identity, contact information, and applied-for gTLD string. Failure to provide any part of this information will result in an application being considered incomplete. Required documents will also be requested and supplied here.

Demonstration of Technical and Operational Capability – These questions are intended to gather information about

an applicant's technical capabilities and plans for operation of the proposed gTLD.

Applicants are not required to have deployed an actual registry to complete the requirements for a successful application. It will be sufficient at application time for an applicant to demonstrate a clear understanding and accomplishment of some groundwork toward the key technical and operational aspects of running a gTLD registry. Each applicant that passes the technical evaluation and all other steps will be required, following execution of a registry agreement, to complete a pre-delegation technical test before delegation of the applied-for gTLD. Refer to Module 5, Transition to Delegation, for additional information.

Demonstration of Financial Capability – These questions are intended to gather information about an applicant's financial capabilities to operate a gTLD registry business and its financial planning in preparation for long-term operation of a new gTLD.

2.1.2.2 Evaluation Methodology

Initial Evaluations are conducted on the basis of the information each applicant makes available to ICANN in its response to the questions in the application form. ICANN and its evaluators are not obliged to take into account any information or evidence that is not made available in the application and submitted by the due date, unless explicitly requested by the evaluators.

It is the applicant's responsibility to ensure that the questions have been fully answered and the required documentation is attached. Evaluators are entitled, but not obliged, to request further information or evidence from an applicant. The Initial Evaluation period provides for one exchange of information between the applicant and the evaluators.⁶ Any such request will be made solely through TAS, rather than by direct means such as phone, letter, email, or other similar means.

Because different registry types and purposes may justify different responses to individual questions, evaluators will

⁶ Some comments suggested that there was a lack of flexibility in the limitation to one exchange between applicant and evaluators during the Initial Evaluation. The design goal is an efficient and predictable process. The opportunity for one communication is a compromise that reduces the bottlenecking issue that would likely occur in an open-ended dialogue, but does afford the opportunity for an applicant to provide any necessary clarifications.

pay particular attention to the consistency of an application across all criteria. For example, an applicant's scaling plans noting hardware to ensure its capacity to operate at a particular volume level should be consistent with its financial plans to secure the necessary equipment.

2.1.3 Registry Services Review

Concurrent with the string reviews described in subsection 2.1.1, ICANN will review the applicant's proposed registry services. The applicant will be required to provide a list of proposed registry services in its application.

Registry services are defined as:

1. operations of the registry critical to the following tasks: the receipt of data from registrars concerning registrations of domain names and name servers; provision to registrars of status information relating to the zone servers for the TLD; dissemination of TLD zone files; operation of the registry zone servers; and dissemination of contact and other information concerning domain name server registrations in the TLD as required by the registry agreement;
2. other products or services that the registry operator is required to provide because of the establishment of a consensus policy; and
3. any other products or services that only a registry operator is capable of providing, by reason of its designation as the registry operator.

Proposed registry services will be examined to determine if they might raise significant stability or security issues. Examples of services proposed by existing registries can be found at <http://www.icann.org/en/registries/rsep/>. In most cases, these proposed services successfully pass this inquiry.

Registry services currently provided by registries can be found in registry agreement appendices. See <http://www.icann.org/en/registries/agreements.htm>.

A full definition of registry service can be found at <http://www.icann.org/en/registries/rsep/rsep.html> and in the draft registry agreement at <http://www.icann.org/en/topics/new-gtlds/draft-agreement-clean-18feb09-en.pdf>.

The review will include a preliminary determination of whether a proposed registry service requires further

consideration based on whether the registry service may raise significant security or stability issues.

If ICANN's preliminary determination reveals that there may be significant security or stability issues surrounding the proposed service, the application will be flagged for an extended review by the DNS Stability Technical Panel (as performed by experts on the existing RSTEP, see <http://www.icann.org/en/registries/rsep/rstep.html>). This review, if applicable, will occur during the Extended Evaluation period (refer to Section 2.2).

Definitions for security and stability applied in the registry services review are:

Security – an effect on security by the proposed registry service means (1) the unauthorized disclosure, alteration, insertion or destruction of registry data, or (2) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.

Stability – an effect on stability means that the proposed registry service (1) does not comply with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant standards-track or best current practice RFCs sponsored by the IETF, or (2) creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant standards-track or best current practice RFCs and relying on registry operator's delegation information or provisioning services.

2.1.4 Applicant's Withdrawal of an Application

An applicant who does not pass the Initial Evaluation may be permitted to withdraw its application at this stage for a partial refund (refer to subsection 1.5.5 of Module 1).

2.2 Extended Evaluation

An applicant may request an Extended Evaluation if the application has failed to pass the Initial Evaluation elements concerning:

- Demonstration of technical and operational capability (refer to subsection 2.1.2.1). There is no

additional fee for an extended evaluation in this instance.

Demonstration of financial capability (refer to subsection 2.1.2.1). There is no additional fee for an extended evaluation in this instance.

- DNS stability – String review (refer to subsection 2.1.1.3). There is no additional fee for an extended evaluation in this instance.
- DNS stability – Registry services (refer to subsection 2.1.3). Note that this investigation incurs an additional fee (the Registry Services Review Fee) if the applicant wishes to proceed. See Section 1.5 of Module 1 for fee and payment information.

From the time an applicant receives notice of failure to pass the Initial Evaluation, it has 15 calendar days to submit to ICANN the Notice of Request for Extended Evaluation through the online application interface. If the applicant does not explicitly request the Extended Evaluation, and pay any additional fees as applicable, the application will not proceed.

2.2.1 Technical and Operational or Financial Extended Evaluation

The following applies to an Extended Evaluation of an applicant's technical and operational capability or financial capability, as described in subsection 2.1.2.1.

An applicant who has requested Extended Evaluation will again access the online application system and clarify its answers to those questions or sections on which it received a non-passing score. The Extended Evaluation allows one additional exchange of information between the evaluators and the applicant to clarify information contained in the application. This supplemental information will become part of the application. Such communications will include a deadline for the applicant to respond. Applicants may not use the Extended Evaluation period to substitute portions of new information for the information submitted in their original applications.

The same panel that reviewed an application during Initial Evaluation will conduct the Extended Evaluation, using the same criteria as outlined at <http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-clean-18feb09-en.pdf>, to determine

whether the application, now that certain information has been clarified, meets the criteria.⁷

ICANN will notify applicants at the end of the Extended Evaluation period as to whether they have passed. If an applicant passes Extended Evaluation, its application continues to the next stage in the process. If an applicant does not pass Extended Evaluation, the application will proceed no further. No further reviews are available.

2.2.2 DNS Stability -- Extended Evaluation

This section applies to an Extended Evaluation of DNS security or stability issues with an applied-for gTLD string, as described in subsection 2.1.1.3.

If an application is subject to Extended Evaluation, an independent 3-member panel will be formed to review the security or stability issues identified during the Initial Evaluation.

The panel will review the string and determine whether the string fails to comply with relevant standards or creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems, and will communicate its findings to ICANN and to the applicant.

If the panel determines that the string does not comply with relevant technical standards or creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems, the application cannot proceed.

2.2.3 Registry Services Extended Evaluation

This section applies to Extended Evaluation of Registry Services, as described in subsection 2.1.3.

If a proposed registry service has been referred to the Registry Services Technical Evaluation Panel (RSTEP) for an extended review, the RSTEP will form a review team of members with the appropriate qualifications.

The review team will generally consist of 3 members, depending on the complexity of the registry service proposed. In a 3-member panel, the review could be conducted within 30 to 45 days. In cases where a 5-

⁷ Some comments were received indicating a preference for a new panel to perform the Extended Evaluation. ICANN will consult with the evaluators retained for this role for their recommendations on what is standard in analogous situations.

member panel is needed, this will be identified before the extended evaluation starts. In a 5-member panel, the review could be conducted in 45 days or fewer.

The cost of an RSTEP review will be covered by the applicant through payment of the Registry Services Review Fee. Refer to payment procedures in section 1.5 of Module 1. The RSTEP team review will not commence until payment has been received.

If the RSTEP finds that one or more of the applicant's proposed registry services may be introduced without risk of a meaningful adverse effect on security or stability, these services may be included in the applicant's contract with ICANN. If the RSTEP finds that the proposed service would create a risk of a meaningful adverse effect on security or stability, the applicant may elect to proceed with its application without the proposed service, or withdraw its application for the gTLD. In this instance, an applicant has 15 calendar days to notify ICANN of its intent to proceed with the application. If an applicant does not explicitly provide this notice, the application will proceed no further.

2.3 Channels for Communication

Defined channels for technical support or exchanges of information with ICANN and its evaluators will be made available to applicants during the Initial Evaluation and Extended Evaluation periods. Contacting individual ICANN staff members, Board members, or other individuals performing an evaluation role in order to lobby or obtain confidential information is not appropriate. In the interests of fairness and equivalent treatment for all applicants, any such individual contacts will be referred to the appropriate communication channels.

DRAFT - New gTLD Program – Initial Evaluation and Extended Evaluation

