To All Prospective Applicants for New gTLDs:

Since ICANN's founding more than ten years ago as a not-for-profit, multi-stakeholder organization dedicated to coordinating the Internet's unique identifier system, one of its foundational principles has been to promote competition and choice in the domain-name marketplace while ensuring Internet security and stability.

We have been engaging in a detailed and lengthy consultation process with all constituencies of the global Internet community as to how best to introduce new gTLDs. Representatives from a wide variety of stakeholders—governments, individuals, civil society, business and intellectual property constituencies, and the technology community—were engaged in discussions and bottom-up policy development for more than three years. In October 2007, the Generic Names Supporting Organization (GNSO)—one of the groups that coordinate global Internet policy at ICANN—completed its policy development work on new gTLDs and approved a set of recommendations. All this policy development work culminated with ICANN's Board of Directors deciding to adopt the community-developed policy at the ICANN Paris meeting in June 2008. You can see a thorough brief of the policy process and outcomes at http://gnso.icann.org/issues/new-gtlds/.

This consultation process has culminated in the development of the Applicant Guidebook which is designed to guide potential applicants through the new gTLD application process, providing detailed information about the rules, requirements and processes. Versions 1 and 2 of the Applicant Guidebook were published in October 2008, and February 2009, respectively, and a number of excerpts and explanatory memoranda were published in June 2009.

Since version 2 of the Applicant Guidebook was published, a considerable amount of feedback, from a wide range of entities, has been received, either through the online public comment forums, at ICANN meetings in Mexico City and Sydney, and regional meetings held in New York, London, Hong Kong and Abu Dhabi. These comments have been analysed and considered in the context of the GNSO policy recommendations and the ICANN Board resolution to adopt those recommendations. The third draft of the Applicant Guidebook has been developed to reflect and address, to the extent possible, the comments that have been received.

I would like to thank all of the businesses, governments, individuals, communities, and other groups that provided comment. This feedback is an essential element of the implementation planning process for introducing new gTLDs.

We believe that with this third draft, the Applicant Guidebook now contains a number of areas which have matured in development over the past year to a point where the process of continuous iteration and community feedback is essentially complete. Those areas include: evaluation criteria, dispute resolution standards and procedures, and contention resolution procedures. This version also incorporates new elements which address pre-delegation testing, and proposed solutions

Brussels   6 Rond Point Schuman, Bt. 5   B-1040 Brussels   BELGIUM T +32 2 234 7870   F +32 2 234 7848
Marina del Rey   4676 Admiralty Way, Suite 330   Marina del Rey, CA 90292   USA T +1 310 823 9358   F +1 310 823 8649

http://icann.org

identified to mitigate the potential for malicious conduct.

A few remaining issues will continue to be the focus of much discussion and debate to reach completion in forthcoming months, in particular, solutions for trademark protection and registry/registrar vertical separation.

As with previous versions of the Applicant Guidebook, several explanatory memoranda will accompany this version to enable readers to better understand the implementation work.

I also note that studies on root zone scaling and economic analysis, which do not impact on the content of the Applicant Guidebook, but which are related to the introduction of new gTLDs, will continue to be discussed in parallel with this draft of the Applicant Guidebook. The Root Zone Scaling Study Working Group recently released a report for comment; while further work is being undertaken to establish how further economic analysis should be done.

I look forward to receiving comments to this draft of the Applicant Guidebook.

Sincerely

Rod Beckstrom
CEO and President

Brussels   6 Rond Point Schuman, Bt. 5   B-1040 Brussels   BELGIUM   T +32 2 234 7870   F +32 2 234 7848
Marina del Rey   4676 Admiralty Way, Suite 330   Marina del Rey, CA 90292   USA   T +1 310 823 9358   F +1 310 823 8649

http://icann.org

Draft Applicant Guidebook, Version 3

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.

ICANN

2 October 2009

Preamble

New gTLDs have been in the forefront of ICANN's agenda since its creation. The new gTLD program will open up the top level of the Internet's namespace to foster diversity, encourage competition, and enhance the utility of the DNS.

Currently the gTLD namespace consists of 21 gTLDs and 251 ccTLDs operating on various models. Each of the gTLDs has a designated "registry operator" according to a Registry Agreement between the operator (or sponsor) and ICANN. The registry operator is responsible for the technical operation of the TLD, including all of the names registered in that TLD. The gTLDs are served by over 900 registrars, who interact with registrants to perform domain name registration and other related services. The new gTLD program will create a means for prospective registry operators to apply for new gTLDs, and create new options for consumers in the market. When the program launches its first application round, ICANN expects a diverse set of applications for new gTLDs, including IDNs, creating significant potential for new uses and benefit to Internet users across the globe.

The program has its origins in carefully deliberated policy development work by the ICANN community. In October 2007, the Generic Names Supporting Organization (GNSO)—one of the groups that coordinate global Internet policy at ICANN—formally completed its policy development work on new gTLDs and approved a set of 19 policy recommendations. Representatives from a wide variety of stakeholder groups—governments, individuals, civil society, business and intellectual property constituencies, and the technology community— were engaged in discussions for more than 18 months on such questions as the demand, benefits and risks of new gTLDs, the selection criteria that should be applied, how gTLDs should be allocated, and the contractual conditions that should be required for new gTLD registries going forward. The culmination of this policy development process was a decision by the ICANN Board of Directors to adopt the community-developed policy in June 2008. A thorough brief to the policy process and outcomes can be found at http://gnso.icann.org/issues/new-gtlds.

ICANN's work is now focused on implementation: creating an application and evaluation process for new gTLDs that is aligned with the policy recommendations and provides a clear roadmap for applicants. This implementation work is reflected in the drafts of the applicant guidebook that have been released for public comment, and in the explanatory papers giving insight into rationale behind some of the conclusions reached on specific topics. Meaningful community input has led to revisions of the draft applicant guidebook. In parallel, ICANN is establishing the resources needed to successfully launch and operate the program.

This draft of the Applicant Guidebook is the third draft made available for public comment as the work advances through implementation.

For current information, timelines and activities related to the New gTLD Program, please go to http://www.icann.org/en/topics/new-gtld-program.htm.

Table of Contents

Draft Applicant Guidebook, v3

Module 1

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.

2 October 2009

Module 1

Introduction to the gTLD Application Process

This module gives applicants an overview of the process for applying for a new generic top-level domain, and includes instructions on how to complete and submit an application, the supporting documentation an applicant must submit with an application, the fees required and when and how to submit them.

This module also describes the conditions associated with particular types of applications, and the application life cycle.

For more about the origins, history and details of the policy development background to the New gTLD Program, please see http://gnso.icann.org/issues/new-gtlds/.

A glossary of relevant terms is included at the end of this Draft Applicant Guidebook.

Prospective applicants are encouraged to read and become familiar with the contents of this entire module, as well as the others, before starting the application process to make sure they understand what is required of them and what they can expect at each stage of the application evaluation process.

1.1 Application Life Cycle and Timelines

This section provides a description of the stages that an application passes through once it is submitted. Some stages will occur for all applications submitted; others will only occur in specific circumstances. Applicants should be aware of the stages and steps involved in processing applications received.

1.1.1 Application Submission Dates

The application submission period opens at [time] UTC [date].

The application submission period closes at [time] UTC [date].

To receive consideration, all applications must be submitted electronically through the online application system by the close of the application submission period.

An application will not be considered, in the absence of exceptional circumstances, if:

- It is received after the close of the application submission period.

- The application form is incomplete (either the questions have not been fully answered or required supporting documents are missing). Applicants will not ordinarily be permitted to supplement their applications after submission.

- The evaluation fee has not been paid by the deadline. Refer to Section 1.5 for fee information.

ICANN has gone to significant lengths to ensure that the online application system will be available for the duration of the application submission period. In the event that the system is not available, ICANN will provide alternative instructions for submitting applications.

1.1.2   *Application Processing Stages*

This subsection provides an overview of the stages involved in processing an application submitted to ICANN. In Figure 1-1, the shortest and most straightforward path is marked with bold lines, while certain stages that may or may not be applicable in any given case are also shown. A brief description of each stage follows.
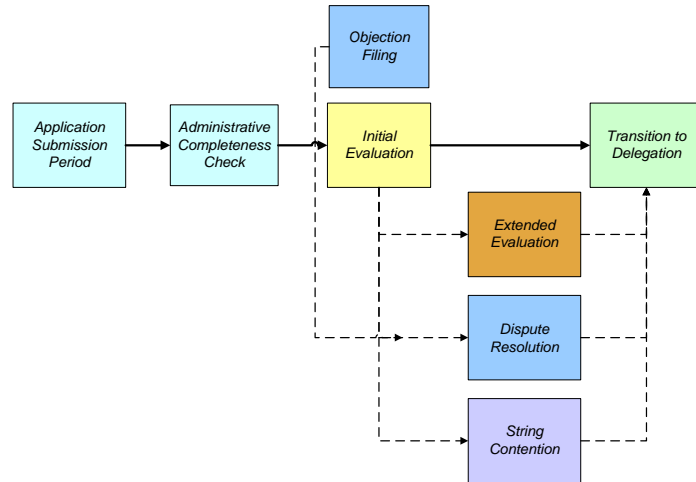
Figure 1-1 – Once submitted to ICANN, applications will pass through multiple stages of processing.

1.1.2.1   *Application Submission Period*

Prior to or at the time the application submission period opens, applicants wishing to apply for a new gTLD can become registered users of the online application system. Information provided in the registration process will be used to validate the identity of the registered user.

Through the application system, applicants will answer a series of questions to provide general information, demonstrate financial capability, and demonstrate technical and operational capability. The supporting documents listed in subsection 1.2.3 of this module must also be submitted through the application system as instructed in the relevant questions.

Applicants must also submit their evaluation fees during this period. Refer to Section 1.5 of this module for additional information about fees and payments.

Following the close of the application period, ICANN will provide applicants with periodic status updates on the progress of their applications.

1.1.2.2   *Administrative Completeness Check*

Immediately following the close of the application submission period, ICANN will check all applications for completeness. This check ensures that:

- All mandatory questions are answered;

- Required supporting documents are provided in the proper format(s); and

- The evaluation fees have been received.

ICANN will post at one time the all applications considered complete and ready for evaluation as soon as practicable after the close of the application period. Certain questions, including finance and security-related questions, have been designated by ICANN as confidential: applicant responses to these questions will not be posted. Confidential questions are labeled as such in the application form. The remainder of the application will be posted.

The administrative completeness check is expected to be completed for all applications in a period of approximately 4 weeks, subject to extension depending on volume. In the event that all applications cannot be processed within a 4-week period, ICANN will post updated process information and an estimated timeline.

1.1.2.3   Initial Evaluation

Initial Evaluation will begin immediately after the administrative completeness check concludes. All complete applications will be reviewed during Initial Evaluation.

There are two main elements of the Initial Evaluation:

1. String reviews (concerning the applied-for gTLD string). String reviews include a determination that the applied-for gTLD string is not likely to cause security or stability problems in the DNS, including problems caused by similarity to existing TLDs or reserved names.

2. Applicant reviews (concerning the entity applying for the gTLD and its proposed registry services). Applicant reviews include a determination of whether the applicant has the requisite technical, operational, and financial capability to operate a registry.

By the conclusion of the Initial Evaluation period, ICANN will post notice of all Initial Evaluation results. Depending on the volume of applications received, ICANN may post such notices in batches over the course of the Initial Evaluation period.

The Initial Evaluation is expected to be completed for all applications in a period of approximately 5 months. If the number of applications is a number in the range of 400, this timeframe would increase by 1-3 months. In this event,

ICANN will construct a method for processing applications in batches, which will extend the time frames involved. In this event, ICANN will post updated process information and an estimated timeline.

1.1.2.4   Objection Filing

Formal objections to applications can be filed on any of four enumerated grounds, by parties with standing to object. The objection filing period will open after ICANN posts the list of complete applications as described in subsection 1.1.2.2.

Objectors must file such formal objections directly with dispute resolution service providers (DRSPs), not with ICANN. Refer to Module 3, Dispute Resolution Procedures, for further details.

The objection filing period will close following the end of the Initial Evaluation period (refer to subsection 1.1.2.3), with a two-week window of time between the posting of the Initial Evaluation results and the close of the objection filing period. Objections that have been filed during the objection filing period will be addressed in the dispute resolution stage, which is outlined in subsection 1.1.2.6 and discussed in detail in Module 3.

All applicants should be aware that third parties have the opportunity to file objections to any application during the objection filing period. Applicants whose applications are the subject of a formal objection will have an opportunity to file a response according to the dispute resolution service provider's rules and procedures (refer to Module 3).

An applicant wishing to file a formal objection to another application that has been submitted would do so within the objection filing period, following the objection filing procedures in Module 3.

1.1.2.5   Extended Evaluation

Extended Evaluation is available only to certain applicants that do not pass Initial Evaluation.

Applicants failing certain elements of the Initial Evaluation can request an Extended Evaluation. If the applicant does not pass Initial Evaluation and does not expressly request an Extended Evaluation, the application will proceed no further. The Extended Evaluation period allows for one additional exchange of information between the applicant and evaluators to clarify information contained in the application. The reviews performed in Extended Evaluation do not introduce additional evaluation criteria.

In addition to failing evaluation elements, an application may be required to enter an Extended Evaluation if the applied-for gTLD string or one or more proposed registry services raise technical issues that might adversely affect the security or stability of the DNS. The Extended Evaluation period provides a time frame for these issues to be investigated. Applicants will be informed if such reviews are required by the end of the Initial Evaluation period.

Evaluators and any applicable experts consulted will communicate the conclusions resulting from the additional review by the end of the Extended Evaluation period.

At the conclusion of the Extended Evaluation period, ICANN will post all evaluator reports from the Initial and Extended Evaluation periods.

If an application passes the Extended Evaluation, it can then proceed to the next relevant stage. If the application does not pass the Extended Evaluation, it will proceed no further.

The Extended Evaluation is expected to be completed for all applications in a period of approximately 5 months, though this timeframe could be increased based on volume. In this event, ICANN will post updated process information and an estimated timeline.

1.1.2.6 Dispute Resolution

Dispute resolution applies only to applicants whose applications are the subject of a formal objection.

Where formal objections are filed and filing fees paid during the objection filing period, independent dispute resolution service providers (DRSPs) will initiate and conclude proceedings based on the objections received. The formal objection procedure exists to provide a path for those who wish to object to an application that has been submitted to ICANN. Dispute resolution service providers serve as the fora to adjudicate the proceedings based on the subject matter and the needed expertise. Consolidation of objections filed will occur where appropriate, at the discretion of the DRSP.

As a result of a dispute resolution proceeding, either the applicant will prevail (in which case the application can proceed to the next relevant stage), or the objector will prevail (in which case either the application will proceed no further or the application will be bound to a contention resolution procedure). In the event of multiple objections, an applicant must prevail in all dispute resolution

proceedings concerning the application to proceed to the next relevant stage. Applicants will be notified by the DRSP(s) of the results of dispute resolution proceedings. Refer to Module 3, Dispute Resolution Procedures, for detailed information.

Dispute resolution proceedings, where applicable, are expected to be completed for all applications within approximately a 5 month time frame. In the event that volume is such that this timeframe cannot be accommodated, ICANN will work with the dispute resolution service providers to create processing procedures and post updated timeline information.

1.1.2.7   String Contention

String contention applies only when there is more than one qualified application for the same or similar gTLD strings.

String contention refers to the scenario in which there is more than one qualified application for the identical gTLD string or for gTLD strings that are so similar that they create a probability of detrimental user confusion if more than one is delegated. String contention cases are resolved either through a community priority (comparative) evaluation (if a community-based applicant elects it) or through an auction.

In the event of contention between applied-for gTLD strings that represent geographical names, the parties may be required to follow a different process to resolve the contention. See subsection 2.1.1.4 of Module 2 for more information.

Groups of applied-for strings that are either identical or confusingly similar are called contention sets. All applicants should be aware that if an application is identified as being part of a contention set, string contention resolution procedures will not begin until all applications in the contention set have completed all aspects of evaluation, including dispute resolution, if applicable.

To illustrate, as shown in Figure 1-2, Applicants A, B, and C all apply for .EXAMPLE and are identified as a contention set. Applicants A and C pass Initial Evaluation, but Applicant B does not. Applicant B requests Extended Evaluation. A third party files an objection to Applicant C's application, and Applicant C enters the dispute resolution process. Applicant A must wait to see whether Applicants B and C successfully complete the Extended Evaluation and dispute resolution phases, respectively, before it can proceed to the string contention resolution stage. In this

example, Applicant B passes the Extended Evaluation, but Applicant C does not prevail in the dispute resolution proceeding. String contention resolution then proceeds between Applicants A and B.
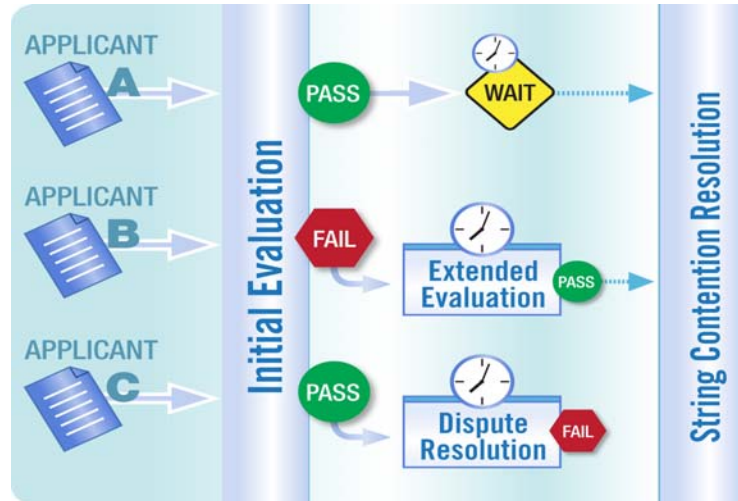
Figure 1-2 – All applications in a contention set must complete all previous evaluation and dispute resolution stages before string contention resolution can begin.

Applicants prevailing in a string contention resolution procedure will proceed toward delegation of the applied-for gTLDs

String contention resolution for a contention set is estimated to take from 2.5 to 6 months to complete. The time required will vary per case because some contention cases may be resolved in either a community priority (comparative) evaluation or an auction, while others may require both processes.

1.1.2.8   Transition to Delegation

Applicants successfully completing all the relevant stages outlined in this subsection 1.1.2 are required to carry out a series of concluding steps before delegation of the applied-for gTLD into the root zone. These steps include execution of a registry agreement with ICANN and completion of a pre-delegation technical test to validate information provided in the application.

Following execution of a registry agreement, the prospective registry operator must complete technical set-up and show satisfactory performance on a set of technical tests before delegation of the gTLD into the root zone may be initiated. If the initial start-up requirements are not satisfied so that the gTLD can be delegated into

the root zone within the time frame specified in the registry agreement, ICANN may in its sole and absolute discretion elect to terminate the registry agreement.

Once all of these steps have been successfully completed, the applicant is eligible for delegation of its applied-for gTLD into the DNS root zone.

It is expected that the transition to delegation steps can be completed in approximately 2 months, though this could take more time depending on the applicant's level of preparedness for the pre-delegation testing.

1.1.2.9 Lifecycle Timelines

Based on the estimates for each stage described in this section, the lifecycle for a straightforward application could be approximately 8 months, as follows:
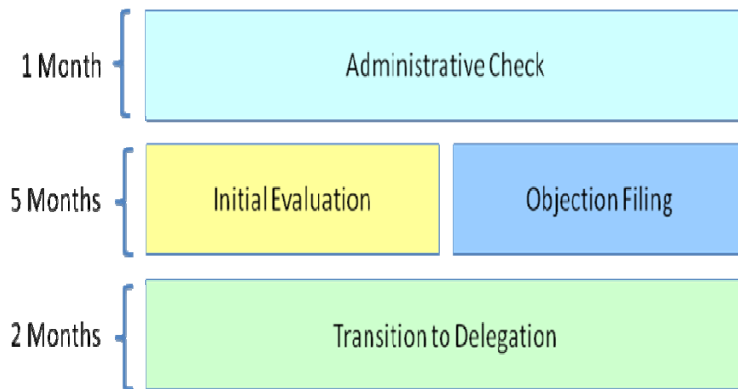
Figure 1-3 – A straightforward application could have an approximate 8-month lifecycle.

The lifecycle for a highly complex application could be much longer, such as 19 months in the example below:
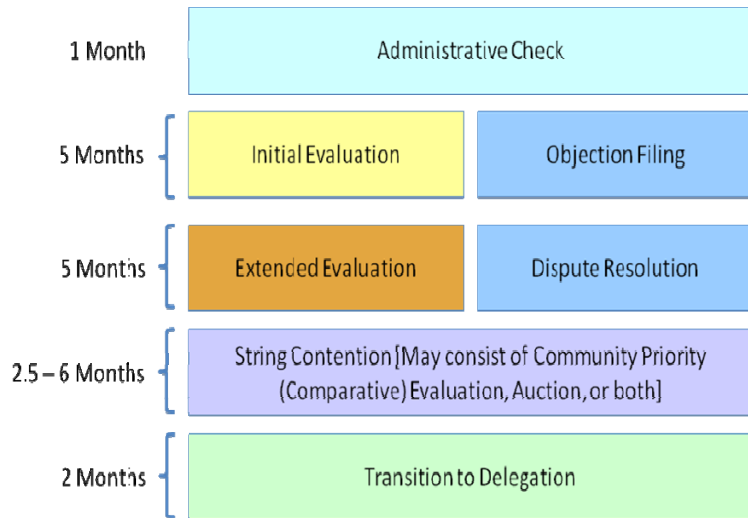
Figure 1-4 – A complex application could have an approximate 19-month lifecycle.

1.1.3 The Role of Public Comment in the Evaluation of Applications

Public comment mechanisms are part of ICANN's policy development and implementation processes. As a private-public partnership, ICANN is dedicated to: preserving the operational security and stability of the Internet, promoting competition, to achieving broad representation of global Internet communities, and developing policy appropriate to its mission through bottom-up, consensus-based processes. This necessarily involves the participation of many stakeholder groups in a public discussion.

In the new gTLD application process, public comments will be a mechanism for the public to bring relevant information and issues to the attention of those charged with handling new gTLD applications. ICANN will open a public comment forum at the time the applications are publicly posted on ICANN's website (refer to subsection 1.1.2.2), which will remain open through the evaluation stages described in subsection 1.1.2. Anyone may submit a comment in the public comment forum.

A distinction should be made between public comments, which may be relevant to ICANN's task of determining whether applications meet the established criteria, and formal objections that concern matters outside those evaluation criteria. The formal objection process was created to allow a full and fair consideration of objections based on limited areas outside ICANN's evaluation of applications on their merits. A party contacting ICANN to

1-10

pursue an objection will be referred to the formal objection channels designed specifically for resolving these matters in the new gTLD application process. More information on the objection and dispute resolution processes is available in Module 3. Public comments received will be provided to the evaluators during the Initial and Extended Evaluation periods. Evaluators will perform take the information provided in these comments into consideration. Consideration of the applicability of the information submitted through public comments will be included in the evaluators' reports.

Public comments may also be relevant to one or more objection grounds. (Refer to Module 3, Dispute Resolution Procedures, for the objection grounds.) ICANN will provide all public comments received to DRSPs, who will have discretion to consider them.

In the event of a community priority (comparative) evaluation (see Module 4, String Contention Procedures), ICANN will provide the comments received to the evaluators with instructions to take the relevant information into account in reaching their conclusions. As the community priority (comparative) evaluation includes assessment of relevant support and opposition, such comments are relevant to the task.

1.1.4   Sample Application Scenarios

The following scenarios briefly show a variety of ways in which an application may proceed through the evaluation process. The table that follows exemplifies various processes and outcomes. This is not intended to be an exhaustive list of possibilities. There are other possible combinations of paths an application could follow.

Estimated time frames for each scenario are also included, based on current knowledge. Actual time frames may vary depending on several factors, including the total number of applications received by ICANN during the application submission period. It should be emphasized that most applications are expected to pass through the process in the shortest period of time, i.e., they will not go through extended evaluation, dispute resolution, or string contention resolution processes. Although most of the scenarios below are for processes extending beyond 8 months, it is expected that most applications will be completed within the eight-month timeframe.

Scenario Number	Initial Eval-uation	Extended Eval-uation	Objec-tion(s) Filed	String Conten-tion	Ap-proved for Dele-gation Steps	Esti-mated Elapsed Time
1	Pass	N/A	None	No	Yes	8 months
2	Fail	Pass	None	No	Yes	13 months
3	Pass	N/A	None	Yes	Yes	10.5 – 14 months
4	Pass	N/A	Applicant prevails	No	Yes	13 months
5	Pass	N/A	Objector prevails	N/A	No	11 months
6	Fail	Quit	N/A	N/A	No	6 months
7	Fail	Fail	N/A	N/A	No	11 months
8	Fail	Pass	Applicant prevails	Yes	Yes	15.5 – 19 months
9	Fail	Pass	Applicant prevails	Yes	No	13.5 – 17 months

Scenario 1 – Pass Initial Evaluation, No Objection, No Contention – In the most straightforward case, the application passes Initial Evaluation and there is no need for an Extended Evaluation. No objections are filed during the objection period, so there is no dispute to resolve. As there is no contention for the applied-for gTLD string, the applicant can enter into a registry agreement and the application can proceed toward delegation of the applied-for gTLD. Most applications are expected to complete the process within this timeframe.

Scenario 2 – Extended Evaluation, No Objection, No Contention – In this case, the application fails one or more aspects of the Initial Evaluation. The applicant is eligible for and requests an Extended Evaluation for the appropriate elements. Here, the application passes the Extended Evaluation. As with Scenario 1, no objections are filed during the objection period, so there is no dispute to resolve. As there is no contention for the gTLD string, the applicant can enter into a registry agreement and the application can proceed toward delegation of the applied-for gTLD.

Scenario 3 – Pass Initial Evaluation, No Objection, Contention – In this case, the application passes the Initial Evaluation so there is no need for Extended Evaluation. No objections are filed during the objection period, so there is no dispute to resolve. However, there are other applications for the same or a similar gTLD string, so there is

contention. In this case, the application wins the contention resolution, and the other contenders are denied their applications, so the winning applicant can enter into a registry agreement and the application can proceed toward delegation of the applied-for gTLD.

Scenario 4 – Pass Initial Evaluation, Win Objection, No Contention – In this case, the application passes the Initial Evaluation so there is no need for Extended Evaluation. During the objection filing period, an objection is filed on one of the four enumerated grounds by an objector with standing (refer to Module 3, Dispute Resolution Procedures). The objection is heard by a dispute resolution service provider panel that finds in favor of the applicant. The applicant can enter into a registry agreement and the application can proceed toward delegation of the applied-for gTLD.

Scenario 5 – Pass Initial Evaluation, Lose Objection – In this case, the application passes the Initial Evaluation so there is no need for Extended Evaluation. During the objection period, multiple objections are filed by one or more objectors with standing for one or more of the four enumerated objection grounds. Each objection is heard by a dispute resolution service provider panel. In this case, the panels find in favor of the applicant for most of the objections, but one finds in favor of the objector. As one of the objections has been upheld, the application does not proceed.

Scenario 6 – Fail Initial Evaluation, Applicant Withdraws – In this case, the application fails one or more aspects of the Initial Evaluation. The applicant decides to withdraw the application rather than continuing with Extended Evaluation. The application does not proceed.

Scenario 7 – Fail Initial Evaluation, Fail Extended Evaluation -- In this case, the application fails one or more aspects of the Initial Evaluation. The applicant requests Extended Evaluation for the appropriate elements. However, the application fails Extended Evaluation also. The application does not proceed.

Scenario 8 – Extended Evaluation, Win Objection, Pass Contention – In this case, the application fails one or more aspects of the Initial Evaluation. The applicant is eligible for and requests an Extended Evaluation for the appropriate elements. Here, the application passes the Extended Evaluation. During the objection filing period, an objection is filed on one of the four enumerated grounds by an objector with standing. The objection is heard by a dispute

resolution service provider panel that finds in favor of the applicant. However, there are other applications for the same or a similar gTLD string, so there is contention. In this case, the applicant prevails over other applications in the contention resolution procedure, the applicant can enter into a registry agreement, and the application can proceed toward delegation of the applied-for gTLD.

Scenario 9 – Extended Evaluation, Objection, Fail Contention – In this case, the application fails one or more aspects of the Initial Evaluation. The applicant is eligible for and requests an Extended Evaluation for the appropriate elements. Here, the application passes the Extended Evaluation. During the objection filing period, an objection is filed on one of the four enumerated grounds by an objector with standing. The objection is heard by a dispute resolution service provider that rules in favor of the applicant. However, there are other applications for the same or a similar gTLD string, so there is contention. In this case, another applicant prevails in the contention resolution procedure, and the application does not proceed.

Transition to Delegation – After an application has successfully completed Initial Evaluation, and other stages as applicable, the applicant is required to complete a set of steps leading to delegation of the gTLD, including execution of a registry agreement with ICANN, and completion of pre-delegation testing. Refer to Module 5 for a description of the steps required in this stage.

1.1.5   Subsequent Application Rounds

ICANN's goal is to launch subsequent gTLD application rounds as quickly as possible. The exact timing will be based on experiences gained and changes required after this round is completed. The goal is for the next application round to begin within one year of the close of the application submission period for this round.

1.2   Information for All Applicants

1.2.1   Eligibility

Any established corporation, organization, or institution in good standing may apply for a new gTLD. Applications from individuals or sole proprietorships will not be considered.

Note that ICANN may deny an otherwise qualified application if:

a. Applicant, or any partner, officer, director, or manager, or any person or entity owning (or beneficially owning) fifteen percent or more of applicant:

    i. within the past ten years, has been convicted of a felony, or of a misdemeanor related to financial or corporate governance activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that ICANN deemed as the substantive equivalent of any of these;

    ii. within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of the funds of others;

    iii. is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in (a) or (b);

    iv. is the subject of a disqualification imposed by ICANN and in effect at the time the application is considered; or

    v. fails to provide ICANN with the identifying information necessary to confirm identity at the time of application.

b. Applicant, or any partner, officer, director, or manager, or any person or entity owning (or beneficially owning) fifteen percent or more of applicant is the subject of a pattern of decisions indicating liability for, or repeated practice of bad faith in regard to domain name registrations, including:

    i. acquiring domain names primarily for the purpose of selling, renting, or otherwise transferring the domain name registrations to the owner of a trademark or service mark or to a competitor, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or

ii. registering domain names in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name; or

iii. registering domain names primarily for the purpose of disrupting the business of a competitor; or

iv. using domain names with intent to attract, for commercial gain, Internet users to a web site or other on-line location, by creating a likelihood of confusion with a trademark or service mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product or service on the web site or location.

1.2.2 Required Documents

All applicants should be prepared to submit the following documents, which are required to accompany each application:

1. **Proof of legal establishment –** Documentation of the applicant's establishment as a specific type of entity in accordance with the applicable laws of its jurisdiction.

2. **Proof of good standing** – Documentation from the applicable body in the applicant's jurisdiction that the applicant is in good standing.

   Under some laws or jurisdictions, it may be possible to prove both establishment and good standing with a single document. That is, the same document may suffice for items 1 and 2.

   The documents supplied for proof of establishment and good standing should constitute a coherent response for the applicant's jurisdiction.

3. **Financial statements**. Applicants must provide audited or certified financial statements for the most recently completed fiscal year for the applicant. In some cases, unaudited financial statements may be provided. Refer to the Evaluation Criteria, attached to Module 2, for details.

All documents must be valid at the time of submission.

Supporting documentation should be submitted in the original language. English translations are not required.

Some types of supporting documentation are required only in certain cases:

1. *Community endorsement –* If an applicant has designated its application as community-based (see section 1.2.3), it will be asked to submit a written endorsement of its application by one or more established institutions representing the community it has named. An applicant may submit written endorsements from multiple institutions. If applicable, this will be submitted in the section of the application concerning the community-based designation.

2. *Government support or non-objection* – If an applicant has applied for a gTLD string that is a geographical name, the applicant is required to submit a statement of support for or non-objection to its application from the relevant governments or public authorities. Refer to subsection 2.1.1.4 for more information on the requirements for geographical names.

3. *Documentation of third-party funding commitments –* If an applicant lists funding from third parties in its application, it must provide evidence of commitment by the party committing the funds. If applicable, this will be submitted in the financial section of the application.

1.2.3   Community-Based Designation

All applicants are required to designate whether their application is **community-based**.

1.2.3.1   Definitions

For purposes of this Applicant Guidebook, a **community-based gTLD** is a gTLD that is operated for the benefit of a clearly delineated community. Designation or non-designation of an application as community-based is entirely at the discretion of the applicant. Any applicant may designate its application as community-based; however, each applicant making this designation is asked to substantiate its status as representative of the community it names in the application. Additional information may be requested in the event of a community priority (comparative) evaluation (refer to Section 4.2 of Module 4). An applicant for a community-based gTLD is expected to:

1. Demonstrate an ongoing relationship with a clearly delineated community.

2. Have applied for a gTLD string strongly and specifically related to the community named in the application.

3. Have proposed dedicated registration and use policies for registrants in its proposed gTLD, commensurate with the community-based purpose it has named.

4. Have its application endorsed in writing by one or more established institutions representing the community it has named.

For purposes of differentiation, an application that has not been designated as community-based will be referred to hereinafter in this document as a **standard application.** A standard gTLD can be used for any purpose consistent with the requirements of the application and evaluation criteria, and with the registry agreement. A standard applicant may or may not have a formal relationship with an exclusive registrant or user population. It may or may not employ eligibility or use restrictions. Standard simply means here that the applicant has not designated the application as community-based.[1]

1.2.3.2 *Implications of Application Designation*

Applicants should understand how their designation as community-based or standard will affect application processing at particular stages, and, if the application is successful, execution of the registry agreement and subsequent obligations as a gTLD registry operator, as described in the following paragraphs.

Objection/Dispute Resolution – All applicants should understand that an objection may be filed against any application on community grounds, even if the applicant has not designated itself as community-based or declared the gTLD to be aimed at a particular community. Refer to Module 3, Dispute Resolution Procedures.

String Contention – Resolution of string contention may include one or more components, depending on the composition of the contention set and the elections made by community-based applicants.

- A **settlement between the parties** can occur at any time after contention is identified. The parties will be encouraged to meet with an objective to settle the contention. Applicants in contention always have the opportunity to resolve the contention voluntarily

---

[1] The term "standard" here replaces the previous terminology of "open" for applications not designated as community-based. "Open" was generally seen as misleading, since an "open" application could in fact impose tight restrictions on registration in its TLD.

resulting in the withdrawal of one or more applications, before reaching the contention resolution stage.

- A **community priority (comparative) evaluation** will take place only if a community-based applicant in a contention set elects this option. All community-based applicants will be offered this option in the event that there is contention remaining after the applications have successfully completed all previous evaluation stages.

- An **auction** will result in cases of contention not resolved by community priority (comparative) evaluation or agreement between the parties. Auction occurs as a contention resolution means of last resort. If a community priority (comparative) evaluation occurs but does not produce a clear winner, an auction will take place to resolve the contention.

Refer to Module 4, String Contention Procedures, for detailed discussions of contention resolution procedures.

Contract Execution and Post-Delegation – A community-based gTLD applicant will be subject to certain post-delegation contractual obligations to operate the gTLD in a manner consistent with the restrictions associated with its community-based designation. ICANN must approve all material changes to the contract, including changes to community-based nature of the gTLD and any associated provisions.

Community-based applications are intended to be a narrow category, for applications where there are distinct associations among the applicant, the community served, and the applied-for gTLD string. Evaluation of an applicant's designation as community-based will occur only in the event of a contention situation that results in a community priority (comparative) evaluation. However, any applicant designating its application as community-based will, if the application is approved, be bound by the registry agreement to implement the community-based restrictions it has specified in the application. This is true even if there are no contending applicants.

1.2.3.3   *Changes to Application Designation*

An applicant may not change its designation as standard or community-based once it has submitted a gTLD application for processing.

1.2.4 Notice concerning Technical Acceptance Issues with New gTLDs

All applicants should be aware that approval of an application and entry into a registry agreement with ICANN do not guarantee that a new gTLD will immediately function throughout the Internet. Past experience indicates that network operators may not immediately fully support new top-level domains, even when these domains have been delegated in the DNS root zone, since third-party software modification may be required and may not happen immediately.

Similarly, software applications sometimes attempt to validate domain names and may not recognize new or unknown top-level domains. ICANN has no authority or ability to require that software accept new top-level domains although it does prominently publicize which top-level domains are valid and has developed a basic tool to assist application providers in the use of current root-zone data.

ICANN encourages applicants to familiarize themselves with these issues and account for them in their startup and launch plans. Successful applicants may find themselves expending considerable efforts working with providers to achieve acceptance of their new top-level domain.

Applicants should review http://www.icann.org/en/topics/TLD-acceptance/ for background. IDN applicants should also review the material concerning experiences with IDN test strings in the root zone (see http://idn.icann.org/).

1.2.5 Terms and Conditions

All applicants must agree to a standard set of Terms and Conditions for the application process. The Terms and Conditions are available in Module 6 of this guidebook.

1.2.6 Notice of Changes to Information

If at any time during the evaluation process information previously submitted by an applicant becomes untrue or inaccurate, the applicant must promptly notify ICANN via submission of the appropriate forms. This includes applicant-specific information such as changes in financial position and changes in ownership or control of the applicant. ICANN reserves the right to require a re-evaluation of the application in the event of a material change.

1.2.7 Voluntary Verification for High Security Zones[2]

An applicant for a new gTLD has the option of taking steps to gain a "verified" status by meeting a set of requirements additional to those that are in place for all applicants. If achieved, this status would allow the new gTLD registry operator to display a seal indicating that it is verified as a high-security zone, to enhance consumer awareness and trust.

The verification opportunity is entirely optional. A choice not to pursue verification at the time of the application does not reflect negatively on the applicant nor affect its scores in the evaluation process. The process for verification is entirely independent of the evaluation process and requires submission of a separate request with supporting information.

To achieve verification, the registry operations must be consistent with the following principles:

1.   The registry maintains effective controls to provide reasonable assurance that the security, availability, and confidentiality of systems and information assets supporting critical registry functions (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services) and business operations are maintained.

2.   The registry maintains effective controls to provide reasonable assurance that the processing of core registry functions is authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

3.   The registry maintains effective controls to provide reasonable assurance that the processing of core registrar functions by its registrars is authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

---

[2] This section is newly included in the guidebook, for comment, with additional details to follow.

The processes required to achieve this high-security status include verification of both registry operations and supporting registrar operations. The verification assessment is performed by an independent entity, external to the gTLD evaluation process.

In the event that an applicant wishes to pursue the verification option, it participates in a two-phased process.

(1) Prior to delegation of the new gTLD, the applicant participates in an assessment (Phase 1) to establish that the TLD operator has designed and established appropriate technical and procedural controls for operations, in line with the requirements.

(2) After the new gTLD has been delegated and begins operations, a specified period will be given for the registry operator to implement all the pre-approved processes and controls. There will then be a second verification assessment (Phase 2) that will test the processes, controls, and procedures documented in Phase 1 to validate that the registry is operating as planned. If deficiencies are identified by the independent assessment agency, they will be communicated to the registry operator. The registry operator will have a limited time to resolve the problem before the request for verification will be turned down. The registry operator is free to re-apply for verification at a later time.

In the event that any new gTLD application completes the evaluation and the TLD is delegated, the registry operator may choose at a later point to request verification and would then complete the above tests in one step. That is, an applicant may choose to take the steps to obtain verification after it has completed the evaluation process and is operating its new gTLD, rather than concurrently with the evaluation process.

The controls necessary to support verification are assessed through audit on a periodic basis, to retain the gTLD's verified status.

The applicant will be required to pay additional fees for both phases of the verification process. The fees will be revenue neutral and will likely be paid to a third party directly.

See the explanatory memorandum *A Model for a High Security Zone Verification Program* for a detailed discussion of the verification option for high security zones.

1.3 Information for Internationalized Domain Name Applicants

Some applied-for gTLD strings are expected to be Internationalized Domain Names (IDNs) that require the insertion of IDN-encoded A-labels into the DNS root zone. IDNs are domain names including characters used in the local representation of languages not written with the basic Latin alphabet (a - z), European-Arabic digits (0 - 9), and the hyphen (-).

An applicant for an IDN string must provide accompanying information indicating compliance with the IDNA protocol and other requirements. The IDNA protocol is currently under revision and its documentation can be found at http://tools.ietf.org/wg/idnabis/.

Applicants must provide applied-for gTLD strings in the form of both a **U-label** and an **A-label**.

An A-label is the ASCII form of an IDN label. Every A-label begins with the IDNA ACE prefix, "xn--", followed by a string that is a valid output of the Punycode algorithm, and hence is a maximum of 59 ASCII characters in length. The prefix and string together must conform to all requirements for a label that can be stored in the DNS including conformance to the LDH (host name) rule described in RFC 1034, RFC 1123, and elsewhere.

A U-label is the Unicode form of an IDN label, which a user expects to be displayed.

For example, using the current IDN test string in Cyrillic script, the U-label is <**испытание**> and the A-label is <**xn--80akhbyknj4f>.** An A-label must be capable of being produced by conversion from a U-label and a U-label must be capable of being produced by conversion from an A-label.

Applicants for IDN gTLDs will also be required to provide the following at the time of the application:

1. Short form of string (in English). The applicant will provide a short description of what the string would mean or represent in English.

2. Language of label (ISO 639-1). The applicant will specify the language of the applied-for TLD string, both

according to the ISO's codes for the representation of names of languages, and in English.

3. Script of label (ISO 15924). The applicant will specify the script of the applied-for gTLD string, both according to the ISO codes for the representation of names of scripts, and in English.

4. Unicode code points. The applicant will list all the code points contained in the U-label according to its Unicode form.

5. IDN tables. An IDN table provides the list of characters eligible for registration in domain names according to registry policy. It will contain any multiple characters that can be considered "the same" for the purposes of registrations at the second level ("variant characters"). Once in use by an active TLD registry, tables will be lodged in the IANA Repository of IDN Practices. For additional information, see existing tables at http://iana.org/domains/idn-tables/, and submission guidelines at http://iana.org/procedures/idn-repository.html.

6. Applicants must further demonstrate that they have made reasonable efforts to ensure that the encoded IDN string does not cause any rendering or operational problems. For example, problems have been identified in strings with characters of mixed right-to-left and left-to-right directionality when numerals are adjacent to the path separator (i.e., a dot). If an applicant is applying for a string with known issues, it should document steps that will be taken to mitigate these issues in applications. While it is not possible to ensure that all rendering problems are avoided, it is important that as many as possible are identified early and that the potential registry operator is aware of these issues. Applicants can become familiar with these issues by understanding the IDNA protocol and in particular the proposed new version of the IDNA protocol (see http://www.icann.org/en/topics/idn/rfcs.htm), and by active participation in the IDN wiki (see http://idn.icann.org/) where some rendering problems are demonstrated.

7. **[Optional]** - Representation of label in phonetic alphabet. The applicant may choose to provide its applied-for gTLD string notated according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/). Note that this information will not be evaluated or scored. The information, if provided, will be used as a guide to

ICANN in responding to inquiries or speaking of the application in public presentations.

Note on Variants -- Currently, the gTLD application process is established so that each application is for one string, whether ASCII or IDN. There has been comment that applications for IDN strings should also accommodate variant strings. Discussions on possible methods of managing variants at the top level have indicated that restricting variants from being delegated in the DNS root zone might disenfranchise certain regions that otherwise would benefit greatly from the introduction of IDN TLDs.

Delegating variant TLDs in the root zone without a mechanism for ensuring that the TLDs are treated in a method that guarantees a good user experience is a stability concern related to confusability for end-users. This can be compared to the "companyname.com" situation, where two domain names (one with all Latin characters and the other with mixed Latin and Cyrillic) look identical, but were different technically. Users clicked on the "wrong" address leading to a site different than expected. This activity resulted in a change in the IDN Guidelines, requiring that scripts not be mixed in domain names unless there is a linguistic reason for doing so (e.g., in the case of Japanese that is represented by mixing of four scripts). This is also a requirement for TLDs, but does not solve the variant issue.

At the same time, disallowing or blocking variant TLDs means that some users will have a very difficult time using the IDN TLDs. In some cases it is not possible for the user to know which character he or she is typing. Some keyboards will offer one or another variant character but not both. In this way, without the variant TLDs in the root, communities may be getting error messages when attempting to reach, for example, a web address with a domain name under one of these IDN TLDs. This is not the intent of IDN deployment. Rather, the objective is to help all communities have equal access to the Internet.

Not all variants are visually confusing. To maximize benefit, ICANN has attempted to define variants in a narrow manner, only including variants that are visually confusing. The intent was to allow variant TLDs that are not visually confusable with others to be delegated in the DNS root zone while a stable solution was found to address the variants that are similar.

At this time it is an open question whether stability issues include variant TLDs that look different, and are typed differently, but are used interchangeably for the same term by the users.

Another open question is the content of an agreement between the IDN TLD operator and ICANN requiring that registrations under two variant TLDs be handled (say, in a bundled or aliased manner, following RFC 3747, or a different technical solution) in a certain manner.

Finally, there is the question of whether it is necessary to enforce rules required for the development of IDN Tables. IDN Tables hold information about the characters that should be treated as variants. The TLD operators develop IDN tables. Presently, TLD operators are urged to consider linguistic and writing system issues in their work of defining variants, and cooperate with other TLD operators that offer the same or very similar looking characters. This is not always practically possible, and there are currently no rules about defining variants. There also are no defined dispute mechanisms in cases where communities may disagree on a variant definition.

An implementation support team of technical and linguistic experts is examining this set of issues and expects to publish a proposed solution for managing variants at the top level. The proposed solution would then be available for public comment.

1.4 Submitting an Application

Applicants may complete the application form and submit supporting documents using ICANN's TLD Application System (TAS). To access the system, each applicant must first register as a TAS user.

As TAS users, applicants will be able to provide responses in open text boxes and submit required supporting documents as attachments. Restrictions on the size of attachments as well as the file formats are included in the instructions on the TAS site.

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

1.4.1 Accessing the TLD Application System

The TAS site is located at [URL to be inserted in final version of Applicant Guidebook].

ICANN will take commercially reasonable steps to protect all applicant data submitted from unauthorized access, but cannot warrant against the malicious acts of third parties who may, through system corruption or other means, gain unauthorized access to such data.

1.4.2 Application Form

The application form encompasses a set of 50 questions. An overview of the areas and questions contained in the form is shown here:

No.	General Questions
1	Full legal name of Applicant
2	Principal business address
3	Phone number of Applicant
4	Fax number of Applicant
5	Email address for Applicant
6	Primary Contact: Name, Title, Address, Phone, Fax, Email
7	Secondary Contact: Name, Title, Address, Phone, Fax, Email
8	Proof of legal establishment
9	Proof of good standing
10	Business ID, Tax ID, VAT registration number, or equivalent of Applicant
11	Applicant background: previous convictions, cybersquatting activities
12	Evaluation fee payment confirmation
13	Applied-for gTLD string,
14	IDN string information, if applicable
15	IDN tables, if applicable

1-27

16	Mitigation of IDN operational or rendering problems, if applicable
17	Representation of string in International Phonetic Alphabet (Optional)
18	Is the application for a community-based TLD?
19	If community based, describe elements of community and proposed policies
20	Mission/purpose of the TLD
21	Is the application for a geographical name? If geographical, documents of support required
22	Provide measures for protection of geographical names at second level
23	Registry Services: name and full description of all registry services to be provided
No.	**Technical and Operational Questions**
24	Technical overview of proposed registry
25	Architecture
26	Database capabilities
27	Geographic diversity
28	DNS service compliance
29	SRS performance
30	EPP
31	Security policy
32	IPv6 reachability
33	Whois
34	Registration life cycle
35	Abuse prevention and mitigation
36	Rights protection mechanisms
37	Data backup

38	Escrow
39	Registry continuity
40	Registry transition (Confidential)
41	Failover testing
42	Monitoring and fault escalation processes
43	DNSSEC
44	IDNs (Optional)
No.	**Financial Questions**
45	Financial statements (Confidential)
46	Projections template: costs and funding (Confidential)
47	Costs: setup and operating (Confidential)
48	Funding and revenue (Confidential)
49	Contingency planning: barriers, funds, volumes (Confidential)
50	Continuity: financial instrument (Confidential)

1.4.3   Technical Support

TAS users can refer to the FAQ/knowledge base or contact [email address to be inserted in final version of Applicant Guidebook] for technical help using the system. Users can expect to receive a tracking ticket number for a technical support request, and a response within 24 to 48 hours through the TAS submission tool.

1.4.4   Backup Application Process

If the online application system is not available, ICANN will provide alternative instructions for submitting applications.

1.5   Fees and Payments

This section describes the fees to be paid by the applicant. Payment instructions are also included here.

1-29

1.5.1   gTLD Evaluation Fee

The gTLD evaluation fee is required from all applicants. This fee is in the amount of USD 185,000. ICANN will not begin its evaluation of an application unless it has received the gTLD evaluation fee by [time] UTC [date]. The gTLD evaluation fee is set to recover costs associated with the new gTLD program. The fee is set to ensure that the program is fully funded and revenue neutral and is not subsidized by existing contributions from ICANN funding sources, including generic TLD registries and registrars, ccTLD contributions and RIR contributions.

The gTLD evaluation fee covers all required reviews in Initial Evaluation and, in most cases, any required reviews in Extended Evaluation. If an extended Registry Services review takes place, an additional fee will be incurred for this review (see section 1.5.2). There is no additional fee to the applicant for Extended Evaluation for DNS stability, geographical names, technical and operational, or financial reviews. The evaluation fee also covers community priority (comparative) evaluation fees in cases where the applicant achieves a passing score.

Refunds -- In certain cases, refunds of a portion of the evaluation fee may be available for applications that are withdrawn before the evaluation process is complete. The amount of the refund will depend on the point in the process at which the withdrawal is made, as follows:

Refund Available to Applicant	Percentage of Evaluation Fee	Amount of Refund
After posting of applications until posting of Initial Evaluation results	70%	USD 130,000
After posting Initial Evaluation results	35%	USD 65,000
After the applicant has completed Dispute Resolution, Extended Evaluation, or String Contention Resolution(s)	20%	USD 37,000

Thus, any applicant that has not been successful is eligible for at least a 20% refund of the evaluation fee if it withdraws its application.

An applicant that wishes to withdraw an application must submit the required form to request a refund, including agreement to the terms and conditions for withdrawal. Refunds will only be issued to the organization that submitted the original payment. All refunds are paid by wire transfer. Any bank transfer or transaction fees incurred by ICANN will be deducted from the amount paid.

Note on 2000 proof-of-concept round applicants --
Participants in ICANN's proof-of-concept application process in 2000 may be eligible for a credit toward the evaluation fee. The credit is in the amount of USD 86,000 and is subject to:

- submission of documentary proof by the applicant that it is the same entity, a successor in interest to the same entity, or an affiliate of the same entity that applied previously;

- a confirmation that the applicant was not awarded any TLD string pursuant to the 2000 proof of concept application round and that the applicant has no legal claims arising from the 2000 proof of concept process; and

- submission of an application, which may be modified from the application originally submitted in 2000, for the same TLD string that such entity applied for in the 2000 proof-of-concept application round.

Each participant in the 2000 proof-of-concept application process is eligible for at most one credit. A maximum of one credit may be claimed for any new gTLD application submitted according to the process in this guidebook. Eligibility for this credit is determined by ICANN.

1.5.2 Fees Required in Some Cases

Applicants may be required to pay additional fees in certain cases where specialized process steps are applicable. Those possible additional fees include:

- ***Registry Services Review Fee –*** If applicable, this fee is payable for additional costs incurred in referring an application to the RSTEP for an extended review. Applicants will be notified if such a fee is due. The fee for a three member RSTEP review team is anticipated to be USD 50,000. In some cases, five-member panels might be required, or there might

be increased scrutiny at a greater cost. In every case, the applicant will be advised of the cost before initiation of the review. Refer to subsection 2.1.3 of Module 2 on Registry Services review.

- *Dispute Resolution Filing Fee –* This amount must accompany any filing of a formal objection and any response that an applicant files to an objection. This fee is payable to the applicable dispute resolution service provider in accordance with the provider's payment instructions. ICANN estimates that non-refundable filing fees could range from approximately USD 1,000 to USD 5,000 (or more) per party per proceeding. Refer to the appropriate provider for the relevant amount. Refer to Module 3 for dispute resolution procedures.

- *Dispute Resolution Adjudication Fee –* This fee is payable directly to the applicable dispute resolution service provider in accordance with that provider's procedures and schedule of costs. Ordinarily, both parties in the dispute resolution proceeding will be required to submit an advance payment of costs in an estimated amount to cover the entire cost of the proceeding. This may be either an hourly fee based on the estimated number of hours the panelists will spend on the case (including review of submissions, facilitation of a hearing, if allowed, and preparation of a decision), or a fixed amount. In cases where disputes are consolidated and there are more than two parties involved, the advance payment of fees will occur according to the dispute resolution service provider's rules.

  The prevailing party in a dispute resolution proceeding will have its advance payment refunded, while the non-prevailing party will not receive a refund and thus will bear the cost of the proceeding. In cases where disputes are consolidated and there are more than two parties involved, the refund of fees will occur according to the dispute resolution service provider's rules.

  ICANN estimates that adjudication fees for a proceeding involving a fixed amount could range from USD 2,000 to USD 8,000 (or more) per proceeding. ICANN further estimates that an hourly rate based proceeding with a one-member panel could range from USD 32,000 to USD 56,000 (or more) and with a three-member panel it could

range from USD 70,000 to USD 122,000 (or more). These estimates may be lower if the panel does not call for written submissions beyond the objection and response, and does not allow a hearing. Please refer to the appropriate provider for the relevant amounts or fee structures. Refer also to Section 3.3 of Module 3 for further details.

- *Community Priority (Comparative) Evaluation Fee* – In the event that the applicant participates in a community priority (comparative) evaluation, this fee is payable as a deposit in an amount to cover the cost of the panel's review of that application (currently estimated at USD 10,000). The deposit is payable to the provider appointed to handle community priority (comparative) evaluations. Applicants will be notified if such a fee is due. Refer to Section 4.2 of Module 4 for circumstances in which a community priority (comparative) evaluation may take place. An applicant who scores at or above the threshold for the community priority (comparative) evaluation will have its deposit refunded.

ICANN will notify the applicants of due dates for payment in respect of additional fees (if applicable).This list does not include fees (annual registry fees) that will be payable to ICANN following execution of a registry agreement.

1.5.3   Payment Method

Payments to ICANN should be submitted by **wire transfer**. Instructions for making a payment by wire transfer will be available in TAS.[3]

1.5.4   Requesting an Invoice

The TAS interface allows applicants to request issuance of an invoice for any of the fees payable to ICANN. This service is for the convenience of applicants that require an invoice to process payments.

1.6   Questions about this Applicant Guidebook

For assistance and questions an applicant may have in the process of completing the application form, a question and answer forum will be open for the duration of the

---

[3] Wire transfer has been identified as the preferred method of payment as it offers a globally accessible and dependable means for international transfer of funds. This enables ICANN to receive the fee and begin processing applications as quickly as possible.

application submission period. Applicants who are unsure of the information being sought in a question or the parameters for acceptable documentation are encouraged to communicate these questions before the application is submitted to avoid the need for exchanges with evaluators to clarify information, which extends the timeframe associated with the application.

Questions may be submitted to [email address to be inserted in final version of Applicant Guidebook].   To provide all applicants equitable access to information, ICANN will post all questions and answers in a centralized location on its website.

All requests to ICANN for information about the process or issues surrounding preparation of an application must be submitted in writing to the designated email address. ICANN will not grant requests from applicants for personal or telephone consultations regarding the preparation of an application. Applicants that contact ICANN for clarification about aspects of the application will be referred to the dedicated online question and answer area.

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

DRAFT - New gTLD Program - Evaluation Process

ICANN

```
Application          Application          Applications          Pass Admin       Yes      Applications
period opens    →    period closes   →    reviewed for     →    Check?        →          posted for public
                                          completeness                                    comment
```

No

Ineligible for further review

Objection filing period opens
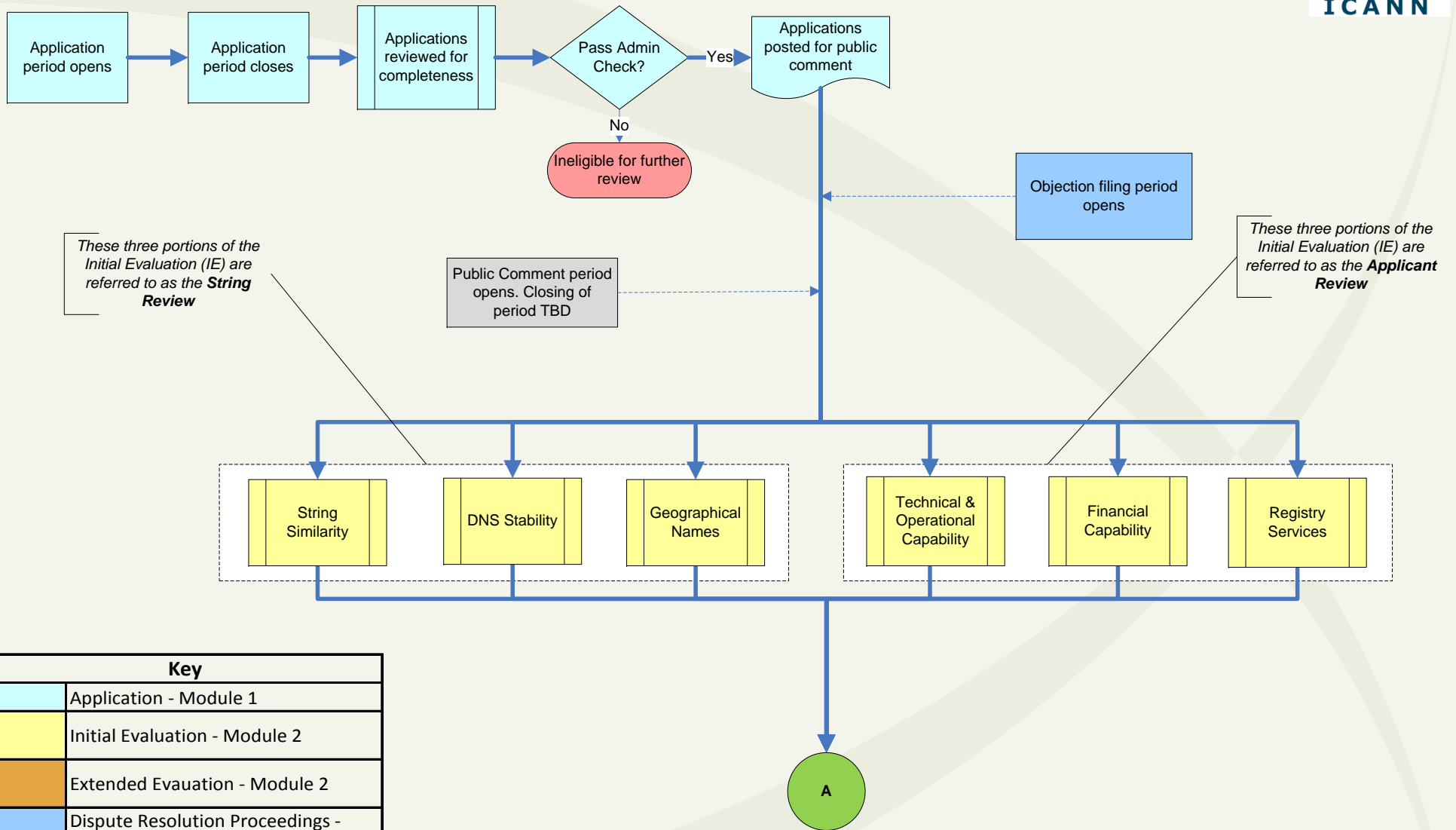
These three portions of the Initial Evaluation (IE) are referred to as the **String Review**

Public Comment period opens. Closing of period TBD

These three portions of the Initial Evaluation (IE) are referred to as the **Applicant Review**

| String Similarity | DNS Stability | Geographical Names |

| Technical & Operational Capability | Financial Capability | Registry Services |

A

Key

	Application - Module 1
	Initial Evaluation - Module 2
	Extended Evauation - Module 2
	Dispute Resolution Proceedings - Module 3
	String Contention - Module 4
	Transition to Delegation - Module 5
Thicker Line	Indicates quickest path to delegation

DRAFT - New gTLD Program - Evaluation Process, Page 2

DRAFT – For Discussion Purposes – Aug 09 – V1.82
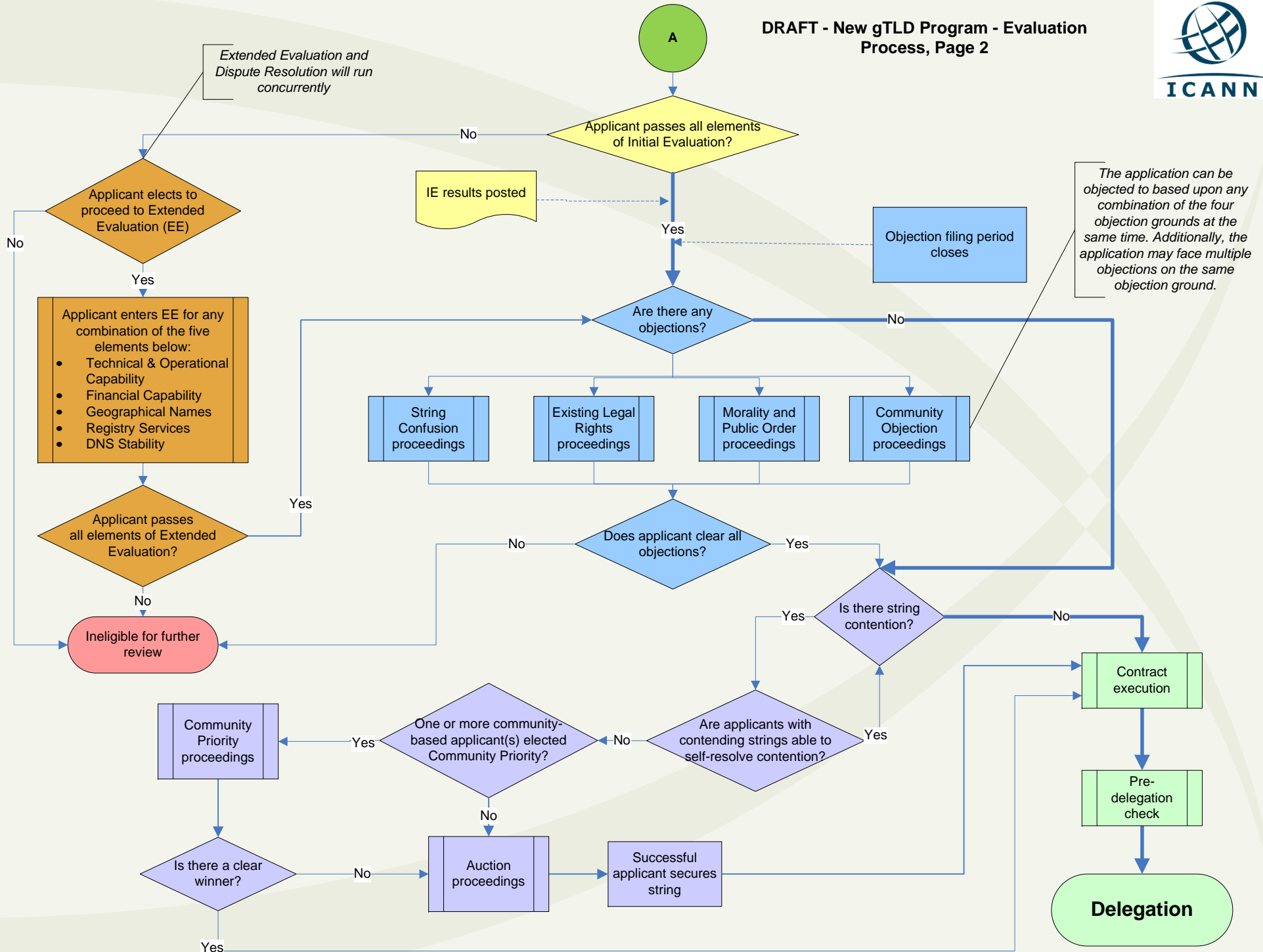
Draft Applicant Guidebook, v3

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.

2 October 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 assesses an applied-for gTLD string, an applicant's qualifications, and its proposed registry services.

The following assessments are performed in the **Initial Evaluation**:

- String Reviews

    - String similarity

    - Reserved names

    - DNS stability

    - Geographical names

- Applicant Reviews

    - Demonstration of technical and operational capability

    - Demonstration of financial capability

    - Registry services reviews for DNS stability issues

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.

String review: 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 evidence of requisite government approval is provided in the case of certain geographical names.

Applicant review: The second review focuses on the applicant to test:

- Whether the applicant has the requisite technical, operational, and financial capability to operate a registry; 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 Similarity Review

This review involves a preliminary comparison of each applied-for gTLD string against existing TLDs and against other applied-for strings. The objective of this review is to prevent user confusion and loss of confidence in the DNS.

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 into 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 an independent String Similarity Panel.

2.1.1.1.1   Review Procedures

The String Similarity Panel's task is to identify visual string similarities that would create a probability of user confusion.

The panel performs this task of assessing similarities that would lead to user confusion in three sets of circumstances, when comparing:

- Applied-for gTLD strings against <u>existing TLDs</u> and reserved names;

- Applied-for gTLD strings against other <u>applied-for gTLD strings;</u> and

- Applied-for gTLD strings against <u>strings requested as IDN ccTLDs.</u>

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

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

In the simple case in which an applied-for gTLD 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).

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 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 of evaluation.

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.

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 a 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. The term "validated" is defined in the IDN ccTLD Fast Track Process Implementation, which can be found at http://www.icann.org/en/topics/idn.

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.

2.1.1.1.2   Review Methodology

The String Similarity Panel is 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 and reserved names. The score will provide one objective measure for consideration by the panel, as part of the process of identifying strings likely to result in user confusion. It should be noted that the score is only indicative and that the final determination of similarity is entirely up to the Panel's judgment.

The algorithm used supports the most common characters in Arabic, Chinese, Cyrillic, Devanagari, Greek, Japanese, Korean, and Latin scripts. It can also compare strings in different scripts to each other.

The algorithm, user guidelines, and additional background information are available to applicants for testing and informational purposes.[1]

The panel will examine all the algorithm data and perform its own review of similarities between strings and whether they rise to the level of string confusion. In cases of strings in scripts not yet supported by the algorithm, the panel's assessment process is entirely manual.

The panel 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.

2.1.1.1.3   Outcomes of the String Similarity Review

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

An application found at risk for string confusion with another applied-for gTLD string will be placed in a contention set.

An application that passes the string similarity 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 string confusion 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.

An applicant may file a formal objection against another gTLD application on string confusion grounds (see Module 3). Such an objection may, if successful, change the configuration of the preliminary contention sets in that the two applied-for gTLD strings will be considered in direct

---

[1] *See* http://icann.sword-group.com/algorithm/

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.

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.

Top-Level Reserved Names List

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

Part I -- Technical Requirements for all Labels (Strings) – The technical requirements for top-level domain labels follow.

1.1 The ASCII label (i.e., the label as transmitted on the wire) must be valid as specified in technical standards *Domain Names: Implementation and Specification* (RFC 1035), and *Clarifications to the DNS Specification* (RFC 2181). This includes the following:

 1.1.1 The label must have no more than 63 characters.

 1.1.2 Upper and lower case characters are treated as identical.

1.2   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:

   1.2.1   The label must consist entirely of letters, digits and hyphens.

   1.2.2   The label must not start or end with a hyphen.

1.3   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. As such, labels:

   1.3.1   Must not be wholly comprised of digits between "0" and "9".

   1.3.2   Must not commence with "0x" or "x," and have the remainder of the label wholly comprised of hexadecimal digits, "0" to "9" and "a" through "f."

   1.3.3   Must not commence with "0o" or "o," and have the remainder of the label wholly comprised of digits between "0" and "7".

1.4   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 as described in Part II).

1.5   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.[2]

---

[2] The primary concern relating to the use of leading- or trailing-numeric labels is due to issues raised by bi-directional scripts when used in conjunction with those labels. Experience has shown that presentation behavior of strings with leading or trailing numbers in bi-directional contexts can be unexpected and can lead to user confusion. As such, a conservative approach is to disallow numerals leading or trailing top-level domain labels.

This concern also applies to all-numeric strings; however, a larger concern with those strings is the risk of confusion and software incompatibilities due to the fact that a top-level domain of all numbers could result in a domain name that is indistinguishable from

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

2.1   The label must be a valid internationalized domain name, as specified in *Internationalizing Domain Names in Applications* (RFC 3490). This includes the following, non-exhaustive, list of limitations:

    2.1.1   Must only contain Unicode code points that are defined as "Valid" in The Unicode Codepoints and IDNA (http://tools.ietf.org/wg/idnabis/), and be accompanied by unambiguous contextual rules where necessary.[3]

    2.1.2   Must be fully compliant with Normalization Form C, as described in *Unicode Standard Annex #15: Unicode Normalization Forms.* See also examples in http://unicode.org/faq/normalization.html.

    2.1.3   Must consist entirely of characters with the same directional property.

2.2   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, non-exhaustive, list of limitations:

    2.2.1   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.

---

an IP address. That is, if (for example) the top-level domain .151 were to be delegated, it would be problematic to programmatically determine whether the string "10.0.0.151" was an IP address or a domain name.

[3] It is expected that the IDNA2008 protocol will be completed and conversion tools will be available before the Application Submission period begins, and that labels will be checked for validity under IDNA2008. In this case, labels valid under the previous version of the protocol (IDNA2003) but not under IDNA2008 will not meet this element of the requirements. Labels that are valid under both versions of the protocol will meet this element of the requirements. Labels valid under IDNA2008 but not under IDNA2003 may meet the requirements; however, applicants are strongly advised to note that the duration of the transition period between the two protocols cannot presently be estimated nor guaranteed in any specific timeframe. The development of support for IDNA2008 in the broader software applications environment will occur gradually. During that time, TLD labels that are valid under IDNA2008, but not under IDNA2003, will have limited functionality.

2.2.2 Exceptions to 2.2.1 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.

Policy Requirements for Generic Top-Level Domains – Applied-for gTLD 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

Applications for gTLD strings must 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 are described in the following paragraphs.

2.1.1.4.1 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 governments or public authorities:

1. An application for any string that is a *country or territory name*. A string shall be considered to be a country or territory name if:

  i. it is an alpha-3 code listed in the ISO 3166-1 standard.

  ii. it is a long-form name listed in the ISO 3166-1 standard, or a translation of the long-form name in any language.

  iii. it is a short-form name listed in the ISO 3166-1 standard, or a translation of the short-form name in any language.

  iv. it is the short- or long-form name association with a code that has been designated as

---

[4] The requirement for gTLD strings to consist of at least three visually distinct characters remains under discussion. An implementation support team of technical and linguistic experts is currently engaging in work on a proposed solution to enable gTLDs of fewer than three characters where appropriate. The proposed solutions will then be made available for public comment.

"exceptionally reserved" by the ISO 3166 Maintenance Agency.

v.   it is a separable component of a country name designated on the "Separable Country Names List," or is a translation of a name appearing on the list, in any language. See the Annex at the end of this module.

vi.   It is a permutation or transposition of any of the names included in items (i) through (v). Permutations include removal of spaces, insertion of punctuation, and addition or removal of grammatical articles like "the." A transposition is considered a change in the sequence of the long or short–form name, for example, "RepublicCzech" or "IslandsCayman."

2.   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 standard.

3.   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.

4.   An application for a *city name*, where the applicant declares that it intends to use the gTLD for purposes associated with the city name.

5.   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.[5]

In the case of an application for a string which represents a continent or UN region, documentation of support will be required from at least 69% of the relevant governments in the region, and there may be no more than one written objection to the application from relevant governments in the region and/or public authorities associated with the continent or the UN region.

An applied-for gTLD string that falls into any the above categories is considered to represent a geographical

---

[5] *See* http://unstats.un.org/unsd/methods/m49/m49regin.htm.

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.

In the event that there is more than one relevant government or public authority for the applied-for gTLD string, the applicant must provide documentation of support or non-objection from all the relevant governments or public authorities.

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 governments or public authorities; 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 should include a signed letter from the relevant government or public authority. Understanding that this will differ across the respective jurisdictions, the letter could be signed by 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; or a senior representative of the agency or department responsible for domain name administration, ICT, foreign affairs, or the Office of the Prime Minister. To assist the applicant in determining who the relevant government or public authority may be for a potential geographic name, the applicant may wish to consult with the relevant Governmental Advisory Committee (GAC) representative.[6]

---

[6] *See* http://gac.icann.org/index.php?name=Representatives&mode=4.

The letter must clearly express the government's or public authority's support for or non-objection to 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. (See Module 5 for a discussion of the obligations of a gTLD registry operator.)

It is important to note that a government or public authority is under no obligation to provide documentation of support or non-objection in response to a request by an applicant.

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.

2.1.1.4.3   Review Procedure for Geographical Names

A Geographic Names Panel (GNP) will confirm whether each applied-for gTLD string represents a geographical name, and verify the relevance and authenticity of the supporting documentation where necessary.

The GNP will review all applications received, not only those where the applicant has noted its applied-for gTLD string as a geographical name. For any applications where the GNP determines that the applied-for gTLD string is not a geographical name, the application will pass the Geographical Names review with no additional steps required.

For any application where the GNP determines that the applied-for gTLD string is a geographical name (as described in this module), the GNP will confirm that the applicant has provided the required 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. In cases where an applicant has not provided the required documentation, the applicant will be contacted and notified of the requirement, and given a limited time frame

to provide the documentation. If the applicant is able to provide the documentation before the close of the Initial Evaluation period, and the documentation is found to meet the requirements, the applicant will pass the geographical names review. If not, the applicant will have additional time to obtain the required documentation; however, if the applicant has not produced the required documentation by the required date, the application will be considered incomplete and will be ineligible for further review. The applicant may reapply in subsequent application rounds, if desired, subject to the fees and requirements of the specific application rounds.

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 Review

In its application, the applicant will respond to a set of questions intended to gather information about the applicant's technical capabilities and its plans for operation of the proposed gTLD.

Applicants are not required to have deployed an actual gTLD registry to pass the Technical/Operational review. It will be necessary, however, for an applicant to demonstrate a clear understanding and accomplishment of some groundwork toward the key technical and operational aspects of a gTLD registry operation. Subsequently, each applicant that passes the technical evaluation and all other steps will be required to complete a pre-delegation technical test prior to delegation of the

new gTLD. Refer to Module 5, Transition to Delegation, for additional information.

2.1.2.2   *Financial Review*

In its application, the applicant will respond to a set of questions intended to gather information about the applicant's financial capabilities for operation of a gTLD registry and its financial planning in preparation for long-term stability of the new gTLD.

Because different registry types and purposes may justify different responses to individual questions, evaluators will pay particular attention to the consistency of an application across all criteria. For example, an applicant's scaling plans identifying system hardware to ensure its capacity to operate at a particular volume level should be consistent with its financial plans to secure the necessary equipment. That is, the evaluation criteria scale with the applicant plans to provide flexibility.

2.1.2.3   *Evaluation Methodology*

Dedicated technical and financial panels of evaluators will conduct the technical/operational and financial reviews, according to the established criteria and scoring methodology included as an attachment to this module. These reviews are conducted on the basis of the information each applicant makes available to ICANN in its response to the questions in the application form.

The evaluators may request clarification or additional information during the Initial Evaluation period. The applicant will have one additional opportunity to clarify or supplement its application in areas requested by the evaluators. These communications will occur via the online application system, rather than by phone, letter, email, or other means. Such communications will include a deadline for the applicant to respond. Any supplemental information provided by the applicant will become part of the application.

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, and 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.

2.1.3 *Registry Services Review*

Concurrent with the other reviews that occur during the Initial Evaluation period, ICANN will review the applicant's proposed registry services for any possible adverse impact on security or stability. The applicant will be required to provide a list of proposed registry services in its application.

2.1.3.1 *Definitions*

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 gTLD 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.

The following registry services are customary services offered by a registry operator:

- Receipt of data from registrars concerning registration of domain names and name servers

- Provision of status information relating to zone servers for the TLD

- Dissemination of TLD zone files

2-16

- Dissemination of contact or other information concerning domain name registrations

- Internationalized Domain Names (if applicable)

- DNS Security Extensions

The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.

Any additional registry services that are unique to the proposed gTLD registry should be described in detail. Directions for describing the registry services are provided at http://www.icann.org/en/registries/rsep/rrs_sample.html.

For purposes of this review, security and stability are defined as follows:

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.

2.1.3.2   *Methodology*

Review of the applicant's proposed registry services will include a preliminary determination of whether any of the proposed registry services raise significant security or stability issues and require additional consideration.

If the preliminary determination reveals that there may be significant security or stability issues (as defined in subsection 2.1.3.1) surrounding a proposed service, the application will be flagged for an extended review by the Registry Services Technical Evaluation Panel (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).

In the event that an application is flagged for extended review of one or more registry services, an additional fee to cover the cost of the extended review will be due from the applicant. Applicants will be advised of any additional fees due, which must be received before the additional review begins.

2.1.4   Applicant's Withdrawal of an Application

An applicant who does not pass the Initial Evaluation may withdraw its application at this stage and request a partial refund (refer to subsection 1.5 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 2.1.2.2). 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.

- 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.

  Geographical names (refer to subsection 2.1.1.4) – There is no additional fee for an extended evaluation in this instance.

An Extended Evaluation does not imply any change of the evaluation criteria. The same criteria used in the Initial Evaluation will be used to review the application in light of clarifications provided by the applicant.

From the time an applicant receives notice of failure to pass the Initial Evaluation, eligible applicants will have 15

calendar days to submit to ICANN the Notice of Request for Extended Evaluation. If the applicant does not explicitly request the Extended Evaluation (and pay an additional fee in the case of a Registry Services inquiry) the application will not proceed.

2.2.1 Technical/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.

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 answers should be responsive to the evaluator report that indicates the reasons for failure. Applicants may not use the Extended Evaluation period to substitute portions of new information for the information submitted in their original applications, i.e., to materially change the application.

An applicant participating in an Extended Evaluation will have the option to have its application reviewed by the same evaluation panelists who performed the review during the Initial Evaluation period, or to have a different set of panelists perform the review during Extended Evaluation.

The Extended Evaluation allows an additional exchange of information between the evaluators and the applicant to further clarify information contained in the application. This supplemental information will become part of the application record. Such communications will include a deadline for the applicant to respond.

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, the DNS Stability Panel will 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-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 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 will 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 such notice within this time frame, the application will proceed no further.

2.3   Parties Involved in Evaluation

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

2.3.1   Panels and Roles

The **String Similarity Panel** assesses whether a proposed gTLD string is likely to result in user confusion due to similarity with any reserved word, any existing TLD, or any new gTLD string applied for in the current application round. This occurs during the String Similarity review in Initial Evaluation.

The **DNS Stability Panel** will review each applied-for string to determine whether the proposed string might adversely affect the security or stability of the DNS. This occurs during the DNS Stability String Review in Initial Evaluation, and may occur again if an applicant does not pass the review in Initial Evaluation and requests Extended Evaluation.

The **Geographical Names Panel** will review each application to determine whether the applied-for gTLD represents a geographic name, as defined in this guidebook. In the event that the string represents a geographic name, the panel will ensure that the required documentation is provided with the application and verify that the documentation is from the relevant governments or public authorities and is authentic.

The **Technical Evaluation Panel** will review the technical components of each application against the criteria in the Applicant Guidebook, along with proposed registry operations, in order to determine whether the applicant is technically and operationally capable of operating a gTLD registry. This occurs during the Technical/Operational Reviews in Initial Evaluation, and may also occur in Extended Evaluation if elected by the applicant.

The **Financial Evaluation Panel** will review each application against the relevant business, financial and organizational criteria contained in the Applicant Guidebook, to determine whether the applicant is financially capable of maintaining a gTLD registry. This occurs during the Financial Review in Initial Evaluation, and may also occur in Extended Evaluation if elected by the applicant.

2-21

The **Registry Services Technical Evaluation Panel (RSTEP)** will review the proposed registry services in the application to determine if any registry services might raise significant security or stability issues. This occurs, if applicable, during the Extended Evaluation period.

Members of these panels are required to abide by the established Code of Conduct and Conflict of Interest guidelines included in this module.

2.3.2   Panel Selection Process

ICANN is in the process of selecting qualified third-party providers to perform the various reviews.[7] In addition to the specific subject matter expertise required for each panel, specified qualifications are required, including:

- The provider must be able to convene – or have the capacity to convene - globally diverse panels and be able to evaluate applications from all regions of the world, including applications for IDN gTLDs.

- The provider should be familiar with the IETF IDNA standards, Unicode standards, relevant RFCs and the terminology associated with IDNs.

- The provider must be able to scale quickly to meet the demands of the evaluation of an unknown number of applications. At present it is not known how many applications will be received, how complex they will be, and whether they will be predominantly for ASCII or non-ASCII gTLDs.

- The provider must be able to evaluate the applications within the required timeframes of Initial and Extended Evaluation.

It is anticipated that the providers will be selected during this year. Additional updates will be posted on ICANN's website.

2.3.3   Code of Conduct Guidelines for Panelists

The purpose of the New gTLD Application Program ("Program") Code of Conduct ("Code") is to prevent real and apparent conflicts of interest and unethical behavior by any Evaluation Panelist ("Panelist").

---

[7] *See* http://icann.org/en/topics/new-gtlds/open-tenders-eoi-en.htm.

Panelists shall conduct themselves as thoughtful, competent, well prepared, and impartial professionals throughout the application process. Panelists are expected to comply with equity and high ethical standards while assuring the Internet community, its constituents, and the public of objectivity, integrity, confidentiality, and credibility. Unethical actions, or even the appearance of compromise, are not acceptable. Panelists are expected to be guided by the following principles in carrying out their respective responsibilities. This Code is intended to summarize the principles and nothing in this Code should be considered as limiting duties, obligations or legal requirements with which Panelists must comply.

Bias -- Panelist shall:

- not advance personal agendas or non-ICANN approved agendas in the evaluation of applications;

- examine facts as they exist and not be influenced by past reputation, media, accounts, etc about the Applicants being evaluated;

- exclude themselves from participating in the evaluation of an application if, to their knowledge, there is some predisposing factor that could prejudice them with respect to such evaluation; and

- exclude themselves from evaluation activities if they are philosophically opposed to or are on record as having made generic criticism about a specific type of Applicant or application

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

If the giving of small tokens is important to the Applicant's culture, Panelists may accept these tokens however, the total of such tokens must not exceed USD 25 in value. If in doubt, the Panelist should err on the side of caution by declining gifts of any kind.

Conflicts of Interest -- Panelists shall act in accordance with the "New gTLD Application Program Conflicts of Interest."

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

Enforcement -- Breaches of this Code, whether intentional or not, shall be reviewed by ICANN, which may make recommendations for corrective action, if deemed necessary. Serious breaches of the Code may be cause for dismissal of the person, persons or provider committing the infraction.

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

2.3.4 Conflict of Interest Guidelines for Panelists

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

To safeguard against the potential for inappropriate influence and ensure applications are evaluated in an objective and independent manner, ICANN has established detailed Conflicts of Interest guidelines and procedures that will be followed by the Evaluation Panelists. To help ensure that the guidelines are appropriately followed ICANN will:

- Require each Evaluation Panelist (provider and individual) to acknowledge and document understanding of the Conflicts of Interest guidelines.

- Identify and secure primary, secondary, and contingent third party providers for each of the evaluation panels highlighted in the Applicant Guidebook.

- In conjunction with the Evaluation Panelists, develop and implement a process to identify conflicts and re-assign applications as appropriate to secondary or contingent third party providers to perform the reviews.

Compliance Period -- All Evaluation Panelists must comply with the Conflicts of Interest guidelines beginning with the opening date of the pre-registration period and ending with the public announcement by ICANN of the final outcomes of all the applications from the Applicant in question.

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

Evaluation Panelists and Immediate Family Members:

- Must not be under contract, have or be included in a current proposal to provide Professional Services for or on behalf of the Applicant during the Compliance Period.

- Must not currently hold or be committed to acquire any interest in a privately-held Applicant

- Must not currently hold or be committed to acquire more than 1% of any publicly listed Applicant's outstanding equity securities or other ownership interests

- Must not be involved or have an interest in a joint venture, partnership or other business arrangement with the Applicant.

- Must not have been named in a lawsuit with or against the Applicant

- Must not be a:

  o Director, officer, or employee, or in any capacity equivalent to that of a member of management of the Applicant;

  o Promoter, underwriter, or voting trustee of the Applicant; or

  o Trustee for any pension or profit-sharing trust of the Applicant.

Definitions--

Evaluation Panelist: An Evaluation Panelist is any individual associated with the review of an application. This includes primary, secondary, and contingent third party Panelists identified through the Expressions of Interest (EOI) process.

Immediate Family Member: Immediate Family Member is a spouse, spousal equivalent, or dependent (whether or not related) of an Evaluation Panelist.

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

2.3.5 Communication Channels

Defined channels for technical support or exchanges of information with ICANN and with evaluation panels 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.

Annex: Separable Country Names List

Under various proposed ICANN policies, eligibility for country name reservation or allocation is tied to listing in property fields of the ISO 3166-1 standard. Notionally, the ISO 3166-1 standard has an "English short name" field which is the common name for a country and can be used for such protections; however, in some cases this does not represent the common name. This registry seeks to add additional protected elements which are derived from definitions in the ISO 3166-1 standard. An explanation of the various classes is included below.

Separable Country Names List

Code	English Short Name	Cl.	Separable Name
ax	Åland Islands	B1	Åland
as	American Samoa	C	Tutuila
		C	Swain's Island
ao	Angola	C	Cabinda
ag	Antigua and Barbuda	A	Antigua
		A	Barbuda
		C	Redonda Island
au	Australia	C	Lord Howe Island
		C	Macquarie Island
		C	Ashmore Island
		C	Cartier Island
		C	Coral Sea Islands
bo	Bolivia, Plurinational State of	B1	Bolivia
ba	Bosnia and Herzegovina	A	Bosnia
		A	Herzegovina
br	Brazil	C	Fernando de Noronha Island
		C	Martim Vaz Islands
		C	Trinidade Island
io	British Indian Ocean Territory	C	Chagos Archipelago
		C	Diego Garcia
bn	Brunei Darussalam	B1	Brunei
		C	Negara Brunei Darussalam
cv	Cape Verde	C	São Tiago
		C	São Vicente
ky	Cayman Islands	C	Grand Cayman
cl	Chile	C	Easter Island
		C	Juan Fernández Islands
		C	Sala y Gómez Island
		C	San Ambrosio Island
		C	San Félix Island
cc	Cocos (Keeling) Islands	A	Cocos Islands
		A	Keeling Islands
co	Colombia	C	Malpelo Island
		C	San Andrés Island
		C	Providencia Island
km	Comoros	C	Anjouan
		C	Grande Comore
		C	Mohéli
ck	Cook Islands	C	Rarotonga
cr	Costa Rica	C	Coco Island
ec	Ecuador	C	Galápagos Islands
gq	Equatorial Guinea	C	Annobón Island
		C	Bioko Island
		C	Río Muni
fk	Falkland Islands (Malvinas)	B1	Falkland Islands
		B1	Malvinas

fo	Faroe Islands	A	Faroe
fj	Fiji	C	Vanua Levu
		C	Viti Levu
		C	Rotuma Island
pf	French Polynesia	C	Austral Islands
		C	Gambier Islands
		C	Marquesas Islands
		C	Society Archipelago
		C	Tahiti
		C	Tuamotu Islands
		C	Clipperton Island
tf	French Southern Territories	C	Amsterdam Islands
		C	Crozet Archipelago
		C	Kerguelen Islands
		C	Saint Paul Island
gr	Greece	C	Mount Athos
gd	Grenada	C	Southern Grenadine Islands
		C	Carriacou
gp	Guadeloupe	C	la Désirade
		C	Marie-Galante
		C	les Saintes
hm	Heard Island and McDonald Islands	A	Heard Island
		A	McDonald Islands
va	Holy See (Vatican City State)	A	Holy See
		A	Vatican
hn	Honduras	C	Swan Islands
in	India	C	Amindivi Islands
		C	Andaman Islands
		C	Laccadive Islands
		C	Minicoy Island
		C	Nicobar Islands
ir	Iran, Islamic Republic of	B1	Iran
ki	Kiribati	C	Gilbert Islands
		C	Tarawa
		C	Banaba
		C	Line Islands
		C	Kiritimati
		C	Phoenix Islands
		C	Abariringa
		C	Enderbury Island
kp	Korea, Democratic People's Republic of	C	North Korea
kr	Korea, Republic of	C	South Korea
la	Lao People's Democratic Republic	B1	Laos
ly	Libyan Arab Jamahiriya	B1	Libya
mk	Macedonia, the Former Yugoslav Republic of	B1	Macedonia
my	Malaysia	C	Sabah
		C	Sarawak
mh	Marshall Islands	C	Jaluit
			Kwajalein
			Majuro
mu	Mauritius	C	Agalega Islands
		C	Cargados Carajos Shoals
		C	Rodrigues Island
fm	Micronesia, Federated States of	B1	Micronesia
		C	Caroline Islands (see also pw)
		C	Chuuk
		C	Kosrae

		C	Pohnpei
		C	Yap
md	Moldova, Republic of	B1	Moldova
		C	Moldava
an	Netherlands Antilles	B1	Antilles
		C	Bonaire
		C	Curaçao
		C	Saba
		C	Saint Eustatius
		C	Saint Martin
nc	New Caledonia	C	Loyalty Islands
mp	Northern Mariana Islands	C	Mariana Islands
		C	Saipan
om	Oman	C	Musandam Peninsula
pw	Palau	C	Caroline islands (see also fm)
		C	Babelthuap
ps	Palestinian Territory, Occupied	B1	Palestine
pg	Papua New Guinea	C	Bismarck Archipelago
		C	Northern Solomon Islands
		C	Bougainville
pn	Pitcairn	C	Ducie Island
		C	Henderson Island
		C	Oeno Island
re	Réunion	C	Bassas da India
		C	Europa Island
		C	Glorioso Island
		C	Juan de Nova Island
		C	Tromelin Island
ru	Russian Federation	B1	Russia
		C	Kaliningrad Region
sh	Saint Helena	C	Gough Island
		C	Tristan de Cunha Archipelago
kn	Saint Kitts and Nevis	A	Saint Kitts
		A	Nevis
pm	Saint Pierre and Miquelon	A	Saint Pierre
		A	Miquelon
vc	Saint Vincent and the Grenadines	A	Saint Vincent
		A	The Grenadines
		C	Northern Grenadine Islands
		C	Bequia
		C	Saint Vincent Island
ws	Samoa	C	Savai'i
		C	Upolu
st	Sao Tome and Principe	A	Sao Tome
		A	Principe
sc	Seychelles	C	Mahé
		C	Aldabra Islands
		C	Amirante Islands
		C	Cosmoledo Islands
		C	Farquhar Islands
sb	Solomon Islands	C	Santa Cruz Islands
		C	Southern Solomon Islands
		C	Guadalcanal
za	South Africa	C	Marion Island
		C	Prince Edward Island
gs	South Georgia and the South Sandwich Islands	A	South Georgia
		A	South Sandwich Islands
sj	Svalbard and Jan Mayen	A	Svalbard

		A	Jan Mayen
		C	Bear Island
sy	Syrian Arab Republic	B1	Syria
tw	Taiwan, Province of China	B1	Taiwan
		C	Penghu Islands
		C	Pescadores
tz	Tanzania, United Republic of	B1	Tanzania
tl	Timor-Leste	C	Oecussi
to	Tonga	C	Tongatapu
tt	Trinidad and Tobago	A	Trinidad
		A	Tobago
tc	Turks and Caicos Islands	A	Turks Islands
		A	Caicos Islands
tv	Tuvalu	C	Fanafuti
ae	United Arab Emirates	B1	Emirates
us	United States	B2	America
um	United States Minor Outlying Islands	C	Baker Island
		C	Howland Island
		C	Jarvis Island
		C	Johnston Atoll
		C	Kingman Reef
		C	Midway Islands
		C	Palmyra Atoll
		C	Wake Island
		C	Navassa Island
vu	Vanuatu	C	Efate
		C	Santo
ve	Venezuela, Bolivarian Republic of	B1	Venezuela
		C	Bird Island
vg	Virgin Islands, British	B1	Virgin Islands
		C	Anegada
		C	Jost Van Dyke
		C	Tortola
		C	Virgin Gorda
vi	Virgin Islands, US	B1	Virgin Islands
		C	Saint Croix
		C	Saint John
		C	Saint Thomas
wf	Wallis and Futuna	A	Wallis
		A	Futuna
		C	Hoorn Islands
		C	Wallis Islands
		C	Uvea
ye	Yemen	C	Socotra Island

Maintenance

A Separable Country Names Registry will be maintained and published by ICANN Staff.

Each time the ISO 3166-1 standard is updated with a new entry, this registry will be reappraised to identify if the changes to the standard warrant changes to the entries in this registry. Appraisal will be based on the criteria listing in the "Eligibility" section of this document.

Codes reserved by the ISO 3166 Maintenance Agency do not have any implication on this registry, only entries derived from normally assigned codes appearing in ISO 3166-1 are eligible.

If an ISO code is struck off the ISO 3166-1 standard, any entries in this registry deriving from that code must be struck.

Eligibility

Each record in this registry is derived from the following possible properties:

Class A:	The ISO 3166-1 English Short Name is comprised of multiple, separable parts whereby the country is comprised of distinct sub-entities. Each of these separable parts is eligible in its own right for consideration as a country name. For example, "Antigua and Barbuda" is comprised of "Antigua" and "Barbuda."
Class B:	The ISO 3166-1 English Short Name (1) or the ISO 3166-1 English Full Name (2) contains additional language as to the type of country the entity is, which is often not used in common usage when referencing the country. For example, one such short name is "The Bolivarian Republic of Venezuela" for a country in common usage referred to as "Venezuela."
Class C:	The ISO 3166-1 Remarks column containing synonyms of the country name, or sub-national entities, as denoted by "often referred to as," "includes", "comprises", "variant" or "principal islands".

In the first two cases, the registry listing must be directly derivative from the English Short Name by excising words and articles. These registry listings do not include vernacular or other non-official terms used to denote the country.

Eligibility is calculated in class order. For example, if a term can be derived both from Class A and Class C, it is only listed as Class A.

DRAFT - New gTLD Program – Initial Evaluation and Extended Evaluation

Application is confirmed as complete and ready for evaluation during Administrative Completeness Check

Initial Evaluation – *String Review*

String Similarity

Application is reviewed to determine if applied-for string is too similar to existing TLDs or Reserved Names

String Similarity Panel compares all applied-for strings and creates contention sets.

DNS Stability

All strings reviewed and in extraordinary cases, ICANN technical experts may determine that string has a strong likelihood of causing DNS instability and will require review during Extended Evaluation

Geographical Names

Geographical Names Panel (GNP) determines if applied-for string is geographical name

GNP confirms supporting documentation where required

Initial Evaluation – *Applicant Review*

Technical and Operational Capability

Evaluators review applicant's answers to questions and supporting documentation

Financial Capability

Evaluators review applicant's answers to questions and supporting documentation

Registry Services

Registry services reviewed, with any services requiring additional review referred to Extended Evaluation.

Extended Evaluation can be for any or all of the five elements below:
- *Technical and Operational Capability*
- *Financial Capability*
- *Geographical Names*
- *DNS Stability*
- *Registry Services*

Does applicant pass all elements of Initial Evaluation? — Yes → **Applicant continues to subsequent steps**

No ↓

Applicant elects to pursue *Extended Evaluation?* — Yes → **Extended Evaluation proceedings**

No ↓

Ineligible for further review

Does applicant pass all elements of Extended Evaluation? — No → **Ineligible for further review** / Yes → **Applicant continues to subsequent steps**

Attachment to Module 2

Evaluation Questions and Criteria

Since ICANN was founded 10 years ago as a not-for-profit, multi-stakeholder organization, one of its key mandates has been to promote competition in the domain name market. ICANN's mission specifically calls for the corporation to maintain and build on processes that will ensure competition and consumer interests – without compromising Internet security and stability. This includes the consideration and implementation of new gTLDs. It is ICANN's goal to make the criteria and evaluation as objective as possible.

While new gTLDs are viewed by ICANN as important to fostering choice, innovation and competition in domain registration services, the decision to launch these coming new gTLD application rounds followed a detailed and lengthy consultation process with all constituencies of the global Internet community.

Any public or private sector organization can apply to create and operate a new gTLD. However the process is not like simply registering or buying a second-level domain name. Instead, the application process is to evaluate and select candidates capable of running a registry, a business that manages top level domains such as, for example, .COM or .INFO. Any successful applicant will need to meet published operational and technical criteria in order to preserve Internet stability and interoperability.

I.   Principles of the Technical and Financial New gTLD Evaluation Criteria

- Principles of conservatism. This is the first round of what is to be an ongoing process for the introduction of new TLDs including Internationalized Domain Names. Therefore, the criteria in this round require applicants to provide a thorough and thoughtful analysis of the technical requirements to operate a registry and the proposed business model.

- The <u>criteria and evaluation should be as objective as possible</u>.

    - With that goal in mind, an important objective of the new TLD process is to <u>diversify the namespace</u>, with different registry business models and target audiences. In some cases, criteria that are objective, but that ignore the differences in business models and target audiences of new registries, will tend to make the process exclusionary. For example, the business model for a registry targeted to a small community need not possess the same robustness in funding and technical infrastructure as a registry intending to compete with large gTLDs. Therefore purely objective criteria such as a requirement for a certain amount of cash on hand will not provide for the flexibility to consider different business models. The process must <u>provide for an objective evaluation framework, but allow for adaptation according to the differing models applicants will present</u>. Within that framework, applicant's responses will be evaluated against the criteria in light of the proposed model.

    - Therefore the <u>criteria should be flexible</u>: able to scale with the overall business approach, providing that the planned approach is consistent and coherent, and can withstand highs and lows.

- Criteria can be <u>objective in areas of registrant protection</u>, for example:
  - Providing for funds to continue operations in the event of a registry failure.
  - Adherence to data escrow and registry failover and continuity plans.

- The evaluation must strike the correct <u>balance</u> between establishing the business and technical competence of the applicant to operate a registry (to <u>serve the interests of registrants</u>), while not asking for the detailed sort of information or making the judgment that a venture capitalist would. ICANN is not seeking to certify business success but instead seeks to encourage innovation while providing certain safeguards for registrants.

- New registries must be added in a way that maintains <u>DNS stability and security</u>. Therefore, ICANN asks several questions so that the applicant can demonstrate an understanding of the technical requirements to operate a registry. In certain cases, ICANN will ask the applicant to demonstrate actual operational technical compliance prior to delegation. This is inline with current prerequisites for the delegation of a TLD.

- <u>Registrant protection</u> is emphasized in both the criteria and the scoring. Examples of this include asking the applicant to:

  - Plan for the <u>occurrence of contingencies and registry failure</u> by putting in place financial resources to fund the ongoing resolution of names while a replacement operator is found or extended notice can be given to registrants,
  - Demonstrate a capability to understand and plan for business contingencies to afford some <u>protections through the marketplace</u>,
  - Adhere <u>to DNS stability and security requirements</u> as described in the technical section, and
  - Provide <u>access</u> to the widest variety of services.

II.   *Aspects of the Questions Asked in the Application and Evaluation Criteria*

The technical and financial questions are intended to inform and guide the applicant in aspects of registry start-up and operation. The established registry operator should find the questions straightforward while inexperienced applicants should find them a natural part of planning.

Evaluation and scoring (detailed below) will emphasize:

- How thorough are the answers? Are they well thought through and do they provide a sufficient basis for evaluation?

- Demonstration of the ability to operate and fund the registry on an ongoing basis:

  - Funding sources to support technical operations in a manner that ensures stability and security and supports planned expenses,
  - Resilience and sustainability in the face of ups and downs, anticipation of contingencies,
  - Bonding or other funding to carry on operations in the event of failure.

- Demonstration that the technical plan will likely deliver on best practices for a registry and identification of issues that might raise DNS stability and security issues.

- Ensures plan integration, consistency and compatibility (responses to questions are not evaluated individually but in comparison to others):
  - Funding adequately covers technical requirements,
  - Funding covers costs,
  - Risks are identified and addressed, in comparison to other aspects of the plan.

III. Scoring

Evaluation

- The questions, criteria, scoring and evaluation methodology are to be conducted in accordance with the principles described earlier in the paper. With that in mind, globally diverse evaluation panelists will staff evaluation panels. The diversity of evaluators and access to experts in all regions of the world will ensure application evaluations take into account cultural, technical and business norms in the regions from which applications originate.

- Evaluation teams will consist of two independent panels. One will evaluate the applications against the financial criteria. The other will evaluate the applications against the technical & operational criteria. Given the requirement that technical and financial planning be well integrated, it is likely that one organization will coordinate the information transfer between panels. Other relevant experts (e.g., technical, audit, legal, insurance, finance) in pertinent regions will provide advice as required.

- Precautions will be taken to ensure that no member of the Evaluation Teams will have any interest or association that may be viewed as a real or potential conflict of interest with an applicant or application. All members must adhere to the Code of Conduct and Conflict of Interest guidelines that are found in Module 2.

- Communications between the evaluation teams and the applicants will be through an online interface. During the evaluation, evaluators may pose a set of clarifying questions to an applicant, to which the applicant may respond through the interface.

- Confidentiality: ICANN will post applications after the close of the application period. The applications consist of the answers to the questions below. The answers to all questions will be published except for the Demonstration of Financial Capability questions (Questions 45 - 50) and the Registry Transition question (40). The answers to these questions will be kept confidential.

Scoring

- Responses will be evaluated against each criterion. A score will be assigned according to the scoring schedule linked to each question or set of questions. In nearly all cases, 2 points are awarded for a response that exceeds requirements, 1 point is awarded for a response that meets requirements and 0 points are awarded for a response that fails to meet requirements. In several questions, 1 point is the maximum score that may be awarded. Each question must receive at least a score of "1," making each a "pass/fail" question.

- In the Continuity question in the financial section(see Question #50), up to 3 points are awarded if an applicant provides, at the application stage, a financial instrument that

will guarantee ongoing registry operations in the event of a business failure. This extra point can serve to guarantee passing the financial criteria for applicants who score the minimum passing score for each of the individual criteria. The purpose of this weighting is to reward applicants who make early arrangements for the protection of registrants and to accept relatively riskier business plans where registrants are protected.

- There are 21 Technical & Operational questions. Each question has a criterion and scoring associated with it. The scoring for each is 0, 1, or 2 points as described above. One of the questions (IDN implementations) is optional. Other than the optional questions, all Technical & Operational criteria must be scored a 1 or more or the application will fail the evaluation.

- The total technical score must be equal to or greater than 22 for the application to pass. That means the applicant can pass by:

  - Receiving a 1 on all questions, including the optional question, and a 2 on at least one mandatory question; or
  - Receiving a 1 on all questions, excluding the optional question and a 2 on at least two mandatory questions.

  This scoring methodology requires a minimum passing score for each question and a slightly higher average score than the per question minimum to pass.

- There are six Financial questions and six sets of criteria that are scored by rating the answers to one or more of the questions. For example, the question concerning registry operation costs requires consistency between the technical plans (described in the answers to the Technical & Operational questions) and the costs (described in the answers to the costs question).

- The scoring for each of the Financial criteria is 0, 1 or 2 points as described above with the exception of the Continuity question, for which up to 3 points are possible. All questions must receive at least a 1 or the application will fail the evaluation.

- The total financial score on the six criteria must be 8 or greater for the application to pass. That means the applicant can pass by:

  - Scoring a 3 on the continuity criteria, or
  - Scoring a 2 on any two financial criteria.

- Applications that do not pass can enter into an extended evaluation process as described in the Applicant Guidebook. The scoring is the same.

	#	Question	Notes	Scoring Range	Criteria	Scoring
Applicant Information	1	Full legal name of the Applicant (the established entity that would enter into a registry agreement with ICANN)	Responses to Questions 1 - 12 are required for a complete application. Responses are not scored.			
	2	Address of the principal place of business of the Applicant. This address will be used for contractual purposes. No Post Office boxes are allowed.				
	3	Phone number for the Applicant's principal place of business.				
	4	Fax number for the Applicant's principal place of business.				
	5	Email address for the Applicant's principal place of business.				
Primary Contact for this Application	6	Name	The primary contact will receive all communications regarding the application. Either the primary or the secondary contact may respond. In the event of a conflict, the communication received from the primary contact will be taken as authoritative.			
		Title				
		Address				
		Phone number				
		Fax number				
		Email address				
Secondary Contact for this Application	7	Name	The secondary contact will be copied on all communications regarding the application. Either the primary or the secondary contact may respond.			
		Title				
		Address				
		Phone number				
		Fax number				
		Email address				
Proof of Legal Establishment	8	(a) Legal form of the Applicant. (e.g., limited liability partnership, corporation, non-profit institution).				
		(b) State the specific national or other jurisdictional law that defines the type of entity identified in 8(a). Identify any relevant section references and provide a URL to the document if available online.				
		(c) Attach evidence of the applicant's establishment as the type of entity identified in Question 8(a) above, in accordance with the applicable laws identified in Question 8(b).	Applications without valid proof of legal establishment will not be evaluated further.			
Proof of Good Standing	9	(a) Identify the specific organizational or business purpose(s) of the entity specified in Question 8.				
		(b) If the applicant operates in a regulated industry where a specific document or license is required to engage in the purpose specified in 9(a) under the laws identified in the applicant's response to question 8(b) (e.g., banking, insurance), the applicant must attach a copy of its current, unrevoked permission or certificate to engage in the activity or operate as the type of business entity identified above. If the applicant's business purpose does not require such permission or certification, the applicant must attach a certificate from the incorporating body or alternative organization authorized by the incorporating body verifying the continued validity of the applicant (e.g., certificate of good standing or affidavit from a notary public). The applicant must clearly explain the chain of authority from the law identified in its response to question 8(b) to the alternative organization providing the documentation.	It may be possible to satisfy this requirement with the document submitted for proof of legal establishment, i.e., the same document may provide both proof of establishment and good standing. In this case, applicant must note so in its response. Applications without valid proof of good standing will not be evaluated further.			
	10	Business ID, Tax ID, VAT registration number, or equivalent of the Applicant.				
Applicant Background	11	(a) Enter the full name, contact information, and position of all directors.	Background checks may be conducted on individuals named in the applicant's response to question 11. Any material misstatement or misrepresentation (or omission of material information) may cause the application to be rejected.			
		(b) Enter the full name, contact information, and position of all officers and partners.				
		(c) Enter the full name, contact information and position of all shareholders holding at least 15% of shares.				

	#	Question	Notes	Scoring Range	Criteria	Scoring
		(d) Indicate whether the applicant or any of its directors, officers, partners, or shareholders named above:	ICANN may deny an otherwise qualified application for any of the following reasons:			
		i. within the past ten years, has been convicted of a felony, or of a misdemeanor related to financial or corporate governance activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that is similar or related to any of these;	Applicant, or any partner, officer, director, or manager, or any person or entity owning (or beneficially owning) fifteen percent or more of applicant:			
		ii. within the past ten years, has been disciplined by a government for conduct involving dishonesty or misuse of funds of others;	a. within the past ten years, has been convicted of a felony, or of a misdemeanor related to financial or corporate governance activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that ICANN deemed as the substantive equivalent of any of these;			
		iii. is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in (i) or (ii); or	b. within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of the funds of others;			
		v. is the subject of a disqualification imposed by ICANN and in effect at the time of this application.	c. is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in (a) or (b);			
		If any of the above events have occurred, please provide details.	d. is the subject of a disqualification imposed by ICANN and in effect at the time the application is considered; or			
			e. fails to provide ICANN with the identifying information necessary to confirm identity at the time of application.			
		(e) Indicate whether the applicant or any of its directors, officers, partners, or shareholders named above have demonstrated a pattern or practice of, or been found liable for, cybersquatting or domain name-related abuses.	ICANN may deny an otherwise qualified application for any of the following reasons: Applicant, or any partner, officer, director, manager, or any person or entity owning (or beneficially owning) fifteen percent or more of applicant is the subject of a pattern of decisions indicating liability for, or repeated practice of bad faith in regard to domain name registrations, including: (i) acquiring domain names primarily for the purpose of selling, renting, or otherwise transferring the domain name registrations to the owner of a trademark or service mark or to a competitor, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or (ii) registering domain names in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name; or (iii) registering domain names primarily for the purpose of disrupting the business of a competitor; or (iv) using domain names with intent to attract, for commercial gain, Internet users to a web site or other on-line location, by creating a likelihood of confusion with a trademark or service mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product or service on the web site or location.			
		(f) Disclose whether the applicant has been involved in any administrative or other legal proceeding in which allegations of intellectual property infringement of a domain name have been made. Provide an explanation related to each such instance.				
Evaluation Fee	12	Enter the confirmation information for your payment of the evaluation fee (e.g., wire transfer confirmation number).				
Applied-for gTLD string	13	Provide the applied-for gTLD string. If applying for an IDN, provide the A-label (beginning with "xn--").	Responses to Questions 13- 17 are not scored, but are used for database and validation purposes.			
	14	(a) If applying for an IDN, provide the U-label.	The U-label is an IDNA-valid string of Unicode characters, including at least one non-ASCII character.			
		(b) If an IDN, provide the translation or transliteration of the string in English, that is, the literal meaning of the string in the opinion of the applicant.				
		(c) If an IDN, provide the language of the label (both in English and as referenced by ISO-639-1).				
		(d) If an IDN, provide the script of the label (both in English and as referenced by ISO 15924).				
		(e) If an IDN, list all the code points contained in the U-label according to Unicode form.				
	15	If an IDN, upload IDN tables for the proposed registry. An IDN table must include: 1) the applied-for gTLD string relevant to the tables, 2) the script or language designator (as defined in BCP 47), 3) table version number, 4) effective date (DD Month YYYY), and 5) contact name, email address, and phone number. Submission of IDN tables in a standards-based format is encouraged.				

	#	Question	Notes	Scoring Range	Criteria	Scoring
	16	If an IDN, describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.				
	17	OPTIONAL. Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).	If provided, this information will be used as a guide to ICANN in communications regarding the application.			
Community-based Designation	18	Is the application for a community-based TLD?	There is a presumption that the application is a standard application (as defined in the Applicant Guidebook) if this question is left unanswered. The applicant's designation as standard or community-based cannot be changed once the application is submitted.			
	19	(a) Provide the name and full description of the community that the applicant is committing to serve. Community-based applications participating in a community priority (comparative) evaluation will be scored in that event based on the community identified in response to this question.	Descriptions should include: • How the community is delineated from Internet users generally. Such descriptions may include, but are not limited to, the following: membership, registration, or licensing processes, operation in a particular industry, use of a language. • How the community is structured and organized. For a community consisting of an alliance of groups, details about the constituent parts are required. • When the community was established, including the date(s) of formal organization, if any, as well as a description of community activities to date. • The current estimated size of the community, both as to membership and geographic extent.		Responses to Question 19 will be regarded as firm commitments to the specified community and reflected in the registry agreement, provided the application is successful. Responses are not scored in the Initial Evaluation. Responses may be scored in a community priority (comparative) evaluation, if applicable. Criteria and scoring methodology for the community priority (comparative) evaluation are described in Module 4 of the Applicant Guidebook.	
		(b) Explain the applicant's relationship to the community identified in 19(a).	Explanations should clearly state: • relations to any community organizations • relations to the community and its constituent parts/groups			
		(c) Provide a description of the community-based purpose of the applied-for gTLD.	Descriptions should include: • Intended registrants in the TLD. • Intended end-users of the TLD. • Related activities the applicant has carried out or intends to carry out in service of this purpose. • Explanation of how the purpose is of a lasting nature. If filled out, this will automatically populate Question 20, on mission/purpose.			
		(d) Explain the relationship between the applied-for gTLD string and the community identified in 19(a).	Explanations should clearly state: • relationship to the established name, if any, of the community. • relationship to the identification of community members. • any connotations the string may have beyond the community.			
		(e) Provide a complete description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD. Policies and enforcement mechanisms are expected to constitute a coherent set.	Descriptions should include proposed policies, if any, on the following: • Eligibility: who is eligible to register a second-level name in the gTLD, and how will eligibility be determined. • Name selection: what types of second-level names may be registered in the gTLD. • Content/Use: what restrictions, if any, the registry operator will impose on how a registrant may use its registered name. • Enforcement: what investigation practices and mechanisms exist to enforce the policies above, what resources are allocated for enforcement, and what appeal mechanisms are available to registrants.			
		(f) Attach any written endorsements for the application from institutions/groups representative of the community identified in 19(a). An applicant may submit endorsements by multiple institutions/groups, if relevant to the community.	Endorsements from institutions/groups not mentioned in the response to 19(b) should be accompanied by a clear description of each such institution's/group's relationship to the community.			
Mission/Purpose	20	Describe the mission/purpose of your proposed gTLD.	Applicants are encouraged to provide a thorough and detailed description to enable informed consultation and comment. Responses to this question are not scored.			
Geographical Names	21	(a) Is the application for a geographical name?	An applied-for gTLD string is considered a geographical name if it is: (a) a country or territory name as defined in the Applicant Guidebook; (b) a sub-national place name listed in the ISO 3166-2 standard; (c) the capital city name of a country or territory listed in the ISO 3166-1 standard; (d) a city name, where the applicant declares in its response to question 20 that it intends to use the gTLD for purposes associated with the city name; or (e) a continent or UN region.			
		(b) If a geographical name, attach documentation of support or non-objection from all relevant governments or public authorities.	See the documentation requirements in Module 2 of the Applicant Guidebook.			

	#	Question	Notes	Scoring Range	Criteria	Scoring
Protection of Geographical Names	22	Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD. This should include any applicable rules and procedures for reservation and/or release of such names.	Applicants should consider and describe how they will incorporate Governmental Advisory Committee (GAC) advice in their management of second-level domain name registrations. See "Principles regarding New gTLDs" at http://gac.icann.org/index.php?name=Imp_doc. For reference, applicants may draw on existing methodology developed for the reservation and release of country names in the .INFO top-level domain. See ".info Procedure" at http://gac.icann.org/index.php?name=Imp_doc. Proposed measures will be posted for public comment as part of the application.			
Registry Services	23	Provide name and full description of all the Registry Services to be provided. Descriptions should include both technical and business components of each proposed service, and address any potential security or stability concerns. The following registry services are customary services offered by a registry operator:

A. Receipt of data from registrars concerning registration of domain names and name servers.
B. Provision of status information relating to zone servers for the TLD.
C. Dissemination of TLD zone files.
D. Dissemination of contact or other information concerning domain name registrations (Whois service).
E. Internationalized Domain Names, where offered.
F. DNS Security Extensions (DNSSEC).
The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.

Additional proposed registry services that are unique to the registry must also be described. | Registry Services are defined as the following: (1) operations of the Registry critical to the following tasks: (i) the receipt of data from registrars concerning registrations of domain names and name servers; (ii) provision to registrars of status information relating to the zone servers for the TLD; (iii) dissemination of TLD zone files; (iv) operation of the Registry zone servers; and (v) dissemination of contact and other information concerning domain name server registrations in the TLD as required by the Registry Agreement; and (2) other products or services that the Registry Operator is required to provide because of the establishment of a Consensus Policy; (3) any other products or services that only a Registry Operator is capable of providing, by reason of its designation as the Registry Operator. A full definition of Registry Services can be found at http://www.icann.org/en/registries/rsep/rsep.html

Security: For purposes of this applicant guidebook, 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 applicable standards.
Stability: For purposes of this applicant guidebook, an effect on stability shall mean that the proposed Registry Service (1) is not compliant 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. | | | |
| **Demonstration of Technical & Operational Capability** | 24 | 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 applicant will provide financial descriptions of resources in the next section and those resources must be reasonably related to these technical requirements.

This high level summary should not repeat answers to questions below. | The questions in this section (24-44) are intended to give applicants an opportunity to demonstrate their technical and operational capabilities to run a registry. In the event that an applicant chooses to outsource one or more parts of its registry operations, the applicant should still provide the full details of the technical arrangements. | 0-2 | Complete answer demonstrates:
(1) complete knowledge and understanding of technical aspects of registry requirements;
(2) an adequate level of resiliency for the registry's technical operations;
(3) consistency with currently deployed technical/operational solutions;
(4) consistency with the overall business approach and planned size of the registry; and
(5) adequate resourcing for technical plan in the planned costs detailed in the financial section. | **2 - exceeds requirements**: Response includes
(1) highly developed and detailed technical plans;
(2) provision of a high level of resiliency;
(3) full interplay and consistency of technical and business requirements; and
(4) evidence of technical resources already on hand or fully committed.
1 - meets requirements: Response includes
(1) adequate level of detail to substantially demonstrate capability and knowledge required to meet this element;
(2) technical plans are commensurate with the overall business approach as described in the application;
(3) demonstrates that technical resources required to carry through the plans for this element are readily available.
0 - fails requirements:
Does not meet the requirements to score 1. |

	#	Question	Notes	Scoring Range	Criteria	Scoring
	25	Architecture: provide details of the system and network architecture that will support the operation of the registry for the proposed scale of the registry. Answers should include information such as: • architecture and network diagrams, • details of hardware and software platforms for DNS and other services, • network bandwidth provision and provider diversity.		0-2	Complete answer demonstrates: (1) detailed and coherent network architecture; (2) architecture providing resiliency for registry systems; (3) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; and (4) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed and detailed network architecture; (2) Evidence of a high level of resiliency, robust and secure infrastructure; (3) Network architecture shows full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or fully committed. **1 - meets requirements**: Response includes (1) Plans for network architecture describe all necessary elements; (2) Descriptions demonstrate adequate network architecture providing robustness and security of the registry; (3) Bandwidth and SLA are commensurate with overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score 1.
	26	Database Capabilities: provide details of database capabilities including: • database software, • storage capacity, • maximum transaction throughput, • scalability, • procedures for object creation, editing, and deletion, • high availability, • change notifications, • registrar transfer procedures, • grace period implementation and • reporting capabilities.		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of database capabilities to meet the registry technical requirements; (2) database capabilities are consistent with the overall business approach, and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Highly developed and detailed description of database capabilities; (2) Evidence of comprehensive database capabilities, including high scalability and redundant database infrastructure, operational and reporting procedures are reviewed regularly and follow leading practices; (3) Database capabilities show full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or fully committed. **1 - meets requirements**: Response includes (1) Plans for database capabilities describe all necessary elements; (2) Descriptions demonstrate adequate database capabilities (not leading practices), with database throughput, scalability, and database operations with limited operational governance. (3) Database capabilities are commensurate with overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score 1.
	27	Geographic Diversity: provide a description of plans for geographic diversity of • name servers and • operations centers. This should include the intended physical locations of systems, operations centers, and other infrastructure. This may include Registry plans to use Anycast or other geo-diversity measures.		0-2	Complete answer demonstrates: (1) geographic diversity of nameservers and operations centers; (2) proposed geo-diversity measures are consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed measures for geo-diversity of operations, with locations and functions; (2) A high level of resiliency, security, and bandwidth; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or committed. **1 - meets requirements**: Response includes (1) Description of geodiversity plans includes all necessary elements; (2) Plans provide adequate geo-diversity of name servers and operations; (3) Geo-diversity plans are commensurate with overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	28	DNS Service Compliance: describe the configuration and operation of nameservers, including how the applicant will comply with 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. Describe the DNS services to be provided, the resources used to implement the services, and demonstrate how the system will function. Suggested information includes: Services. Query rates to be supported at initial operation, and reserve capacity of the system. How will these be scaled as a function of growth in the TLD? Similarly, describe how services will scale for name server update method and performance. Resources. Describe complete server hardware and software. Describe how services are compliant with RFCs. Are these dedicated or shared with any other functions (capacity/performance) or DNS zones? Describe network bandwidth and addressing plans for servers. Describe how the proposed infrastructure will be able to deliver the performance described in the Performance Specification (Specification 6) attached to the draft Registry Agreement. Examples of evidence include: • Server configuration(s) • Network addressing and bandwidth for query load and update propagation	Note that the use of DNS wildcard resource records as described in RFC 4592 or any other method or technology for synthesizing DNS resource records or using redirection within the DNS by the registry is prohibited in the Registry Agreement. Also note that name servers for the new gTLD must comply with IANA Technical requirements for authoritative name servers: http://www.iana.org/procedures/nameserver-requirements.html.	0-2	Complete answer demonstrates: (1) adequate description of configurations of nameservers and compliance with respective DNS protocol-related RFCs; (2) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section; and (4) evidence of compliance with Specification 6 to the Registry Agreement.	2 - exceeds requirements: Response includes: (1) Highly developed and detailed plans to ensure compliance with DNS protocols and required performance specifications; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or committed. 1 - meets requirements: Response includes: (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Plans are sufficient to result in compliance with DNS protocols and required performance specifications; and (3) Plans are commensurate with overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. 0 - fails requirements: Does not meet the requirements to score 1.
	29	SRS Performance: describe the plan for operation of a robust and reliable Shared Registration System. SRS is a critical registry function for enabling multiple registrars to provide domain name registration services in the TLD. Please refer to the requirements in the Registry Interoperability, Continuity, and Performance Specification (Specification 6) attached to the draft Registry Agreement.		0-1	Complete answer demonstrates: (1) a robust plan for operating a reliable SRS; (2) scalability and performance are consistent with the overall business approach, and planned size of the registry; (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section; and (4) evidence of compliance with Specification 6 to the Registry Agreement.	1 - meets requirements: Response includes (1) Evidence of highly developed and detailed plan to operate a robust and reliable; (2) SRS plans are sufficient to result in compliance with the Registry Continuity, Interoperability, and Performance Specifications; (3) Full interplay and consistency of technical and business requirements; and (4) Demonstrates that technical resources are already on hand, or committed or readily available. 0 - fails requirements: Does not meet the requirements to score 1.
	30	EPP: provide a detailed description of the interface with registrars, including how the applicant will comply with Extensible Provisioning Protocol in the relevant RFCs, including but not limited to: RFCs 3915, 3735, and 5730-5734. Provide the EPP templates and schemas that will be used.		0-1	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	1 - meets requirements: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) EPP templates and schemas compliant with RFCs and provide all necessary functionalities for registrar interface; (3) Full interplay and consistency of technical and business requirements; and (4) Demonstrates that technical resources are already on hand, or committed or readily available. 0 - fails requirements: Does not meet the requirements to score 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	31	Security Policy: provide an outline of the security policy and procedures for the proposed registry, including: • system and network access control, ensuring systems are maintained in a secure fashion, including details of how they are monitored, logged and backed up; • 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 and the defenses that will be deployed against those threats; • details for auditing capability on all network access; • independent assessment report to demonstrate security capabilities, if any; • resources to secure integrity of updates between registry systems and nameservers, and between nameservers, if any.		0-2	Complete answer demonstrates: (1) detailed description of processes and solutions deployed to manage logical security across infrastructure and systems, monitoring and detecting threats and security vulnerabilities and taking appropriate steps to resolve them; (2) security capabilities are consistent with the overall business approach and planned size of the registry; (3) a technical plan adequately resourced in the planned costs detailed in the financial section; and (4) security measures are consistent with any commitments made to registrants regarding security levels.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed and detailed security capabilities, with various baseline security levels, independent benchmarking of security metrics, robust periodic security monitoring, and continuous enforcement; (2) Independent assessment report available with leading practices being followed; (3) Full interplay of business and technical requirements; and (4) Evidence of technical resources already on hand or fully committed. **1 - meets requirements**: Response includes: (1) Adequate level of detail to substantially demonstrate capability and knowledge to meet this element; (2) Evidence of adequate security capabilities, enforcement of logical access control, threat analysis, incident response and auditing. Ad-hoc oversight and governance and leading practices being followed; (3) Security capabilities aligned with the overall business approach as described in the application, and any commitments made to registrants; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements**: Does not meet the requirements to score 1.
	32	IPv6 Reachability: the registry supports access to Whois, Web based Whois and any other Registration Data Publication Service as described in Specification 6 to the Registry Agreement. The registry also supports DNS servers over an IPv6 network for at least 2 nameservers. IANA currently has a minimum set of technical requirements for IPv4 name service. These include two nameservers separated by geography and by network topology, each serving a consistent set of data, and are reachable from multiple locations across the globe. Describe how the registry will meet this same criterion for IPv6, requiring IPv6 transport to their network. List all services that will be provided over IPv6, and describe the IPv6 connectivity and provider diversity that will be used.		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed and detailed network architecture and implementation plan, indicating IPv6 reachability allowing IPv6 transport in the network in compliance to IPv4 IANA specifications with at least 2 separated nameservers; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or fully committed. **1 - meets requirements**: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence of adequate implementation plan addressing requirements for IPv6 reachability, including identification of IPv6 reachable nameservers; (3) IPv6 plans commensurate with overall business approach as described in the application; and (4) demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements**: Does not meet the requirements to score 1.
	33	Whois: describe how the applicant will comply with ICANN's Registry Publicly Available Registration Data (Whois) specifications for data objects, bulk access, and lookups as defined in the base agreement: "Specification for Registration Data Publication Services." (Spec 4) Describe how the Applicant's Registry Publicly Available Registration Data (Whois) service will comply with RFC 3912. Describe how the applicant will comply with performance specifications for Whois service as in Specification 6 to the draft registry agreement.		0-1	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**1 - meets requirements**: Response includes (1) adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; and (2) Whois services compliant with RFCs and provide all necessary functionalities for user interface; (3) Whois capabilities commensurate with the overall business approach as described in the application; and (4) demonstrates that technical resources required to carry through the plans for this element are already on hand or readily available. **0 - fails requirements**: Does not meet the requirements to score 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	34	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. It must describe the typical registration lifecycle of create/update/delete and all intervening steps such as pending, locked, expired, and transferred that may apply. Any time elements that are involved - for instance details of add-grace or redemption grace periods, or notice periods for renewals or transfers - must also be clearly explained.		0-1	Complete answer demonstrates: (1) complete knowledge and understanding of registration lifecycles and states; and (2) consistency with any specific commitments made to registrants as adapted to the overall business approach for the proposed gTLD.	1 - meets requirements: Response includes (1) Evidence of highly developed registration life cycle with definition of various registration states and transition between the states; (2) Consistency of registration lifecycle with any commitments to registrants and with technical and financial plans; and (3) Demonstrates that technical resources required to carry through the plans for this element are already on hand or readily available. 0 - fails requirements: Does not meet the requirements to score 1.
	35	Abuse Prevention and Mitigation: Applicants should describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users. Answers should include: • safeguards the applicant will implement at the time of registration, policies to reduce opportunities for abusive behaviors using registered domain names in the TLD, and policies for handling complaints regarding abuse. Each registry operator will be required 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. • a description of rapid takedown or suspension systems that will be implemented. • proposed measures for management and removal of orphan glue records for names removed from the zone.		0-1	Complete answer demonstrates: (1) Comprehensive abuse policies and procedures that will effectively minimize potential for abuse in the TLD; (2) Plans are adequately resourced in the planned costs detailed in the financial section; (3) Policies and procedures identify and address the abusive use of registered names at startup and on an ongoing basis; and (4) When executed in accordance with the Registry Agreement, plans will result in compliance with contractual requirements.	1 - meets requirements: Response includes (1) Evidence of highly developed abuse policies and procedures; (2) Plans are consistent with overall business approach and any commitments made to registrants; and (3) Plans are sufficient to result in compliance with contractual requirements. 0 – fails Requirements: Does not meet the requirements to score 1.
	36	Rights Protection Mechanisms: Applicants should describe how their proposal will create policies and practices that minimize abusive registrations and other activities that affect the legal rights of others. Describe how the proposal will implement safeguards against allowing unqualified registrations, and reduce opportunities for behaviors such as phishing or pharming. Answers may also include additional measures such as abusive use policies, takedown procedures, registrant pre-verification, or authentication procedures, or other covenants.	Note that requirements for rights protection mechanisms remain under discussion. The applicant questions and criteria included here are expected to evolve as a result of community consideration on an effective approach to rights protection in new gTLDs. In this regard, various proposals and corresponding guidebook language are being published for comment simultaneously with the publication of this draft of the Applicant Guidebook.	0-2	Complete answer describes mechanisms designed to: (1) prevent abusive registrations, and (2) identify and address the abusive use of registered names on an ongoing basis.	2 - exceeds requirements: (1) Evidence of highly developed rights protection mechanisms (RPM) specified in detail for inclusion into registry agreement; (2) Mechanisms provide pre-registration and post-registration (beyond UDRP) protections; and (3) Mechanisms address registry start-up and ongoing operations. 1 - meets requirements: Response includes (1) Proposed registry operator commits to and describes rights protection mechanisms; and (2) These mechanisms provide protections at least at registry start-up. 0 - fails requirements: Does not meet the requirements to score 1.
	37	Data Backup: provide • details of frequency and procedures for backup of data, • hardware, and systems used for backup • data format, • data backup features, and • procedures for retrieval of data/rebuild of database.		0-2	Complete answer demonstrates: (1) detailed backup processes deployed, retrieval process and frequency; (2) a backup and retrieval process that is consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	2 - exceeds requirements: Response includes (1) Evidence of highly developed data backup policies and procedures, with continuous robust monitoring, continuous enforcement of backup security, regular review of backups, regular recovery testing, and recovery analysis. Leading practices being followed; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or fully committed. 1 - meets requirements: Response includes (1) Adequate backup procedures, recovery steps, and retrieval capabilities available; (2) Minimal leading practices being followed; (3) Backup procedures commensurate with the overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. 0 - fails requirements: Does not meet the requirements to score a 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	38	Escrow: describe how the applicant will comply with the escrow arrangements documented in the Registry Data Escrow Specifications (Specification 2 of the draft Registry Agreement).		0-2	Complete answer demonstrates: (1) compliance with Specification 2 of the Registry Agreement; (2) a technical plan that is adequately resourced in the planned costs detailed in the financial section; and (3) the escrow arrangement is consistent with the overall business approach and size/scope of the registry.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed and detailed data escrow procedures, including continuous monitoring, archiving, and periodic review for continuous registry operations; (2) Evidences compliance with Specification 2 of the Registry Agreement; (3) Full interplay of technical and business requirements; and (4) Evidence of technical resources already on hand or committed. **1 – meets requirements**: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Data escrow plans are sufficient to result in compliance with the Data Escrow Specification; (3) Escrow capabilities are commensurate with the overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 – fails requirements:** Does not meet the requirements to score a 1.
	39	Registry Continuity: describe how the applicant will comply with registry continuity obligations as described in the Registry Interoperability, Continuity and Performance Specification (Specification 6), attached to the draft Base Agreement.	For reference, applicants should review the ICANN gTLD Registry Continuity Plan at http://www.icann.org/en/registries/continuity/gtld-registry-continuity-plan-25apr09-en.pdf.	0-2	Complete answer demonstrates: (1) detailed description showing plans for compliance with registry continuity obligations; (2) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Highly developed and detailed systems for maintaining registry continuity; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements, and (4) Evidence of technical resources already on hand or committed. **1 - meets requirements**: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Continuity plans are sufficient to result in compliance with requirements; (3) Continuity plans are commensurate with overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements**: Does not meet the requirements to score a 1.
	40	Registry Transition: provide a plan that could be followed in the event that it becomes necessary to transition the proposed gTLD to a new operator, including a transition process. **(Responses to this question will be kept confidential.)**		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements**: Response includes (1) Evidence of highly developed registry transition plan including time required for transitions, feasibility analysis during transition, robust monitoring the pre- and post-delegation phases; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; and (4) A transition provider is already on hand. **1 - meets requirements**: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence of adequate registry transition plan with ad hoc monitoring during registry transition; (3) Transition plan is commensurate with the overall business approach as described in the application; and (4) Resources for registry transition are fully committed. **0 - fails requirements**: Does not meet the requirements to score a 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	41	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, or registry data escrow testing.		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements:** Response includes (1) Evidence of highly developed and detailed failover testing plan, including periodic testing, robust monitoring, review, and analysis; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; (4) Evidence of technical resources for failover testing already on hand or fully committed. **1 - meets requirements:** Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence of adequate failover testing plan with ad hoc review and analysis of failover testing results. (3) Failover testing plan is commensurate with the overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score a 1.
	42	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. Applicant will describe monitoring and communication mechanisms to registrars for detecting and signaling registry entries resulting in DNS response sizes exceeding the common 512-byte threshold and the RFC-3226-mandated 1220-byte threshold once DNSSEC support is provided.		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section; and (4) consistency with the commitments made to registrants regarding system maintenance.	**2 - exceeds requirements:** Response includes (1) Evidence showing highly developed and detailed fault tolerance/monitoring and redundant systems deployed with real-time monitoring tools / dashboard (metrics) deployed and reviewed regularly; (2) A high level of resiliency; (3) Full interplay and consistency of technical and business requirements; and (3) Evidence of technical resources for monitoring and fault escalation already on hand or fully committed. **1 - meets requirements:** Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence showing adequate fault tolerance/monitoring systems planned with ad hoc monitoring and limited periodic review being performed; (3) Plans are commensurate with overall business approach; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score 1.
	43	DNSSEC: Describe 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 how keying material will be securely exchanged and stored. Describe how the DNSSEC implementation will comply with relevant RFCs, including but not limited to: RFCs 4033, 4034, 4035, 4310, 4509, 4641, and 5155 (the latter will only be required if Hashed Authenticated Denial of Existence will be offered).		0-2	Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan scope/scale that is consistent with the overall business approach and planned size of the registry; and (3) a technical plan that is adequately resourced in the planned costs detailed in the financial section.	**2 - exceeds requirements:** Response includes (1) Evidence of highly developed and detailed policies and procedures for offering DNSSEC at time of launch, in compliance with required RFCs, and secure encryption key management (exchange and storage); (2) Key management procedures for registrants in the proposed TLD; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources already on hand or committed. Applicant must also be able to pass requirements for DNSSEC in pre-delegation testing. **1 - meets requirements:** Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence of an adequate DNSSEC implementation plan that provides a high level of resiliency; (3) Technical plan is commensurate with the overall business approach as described in the application; and (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. **0 - fails requirements:** Does not meet the requirements to score 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	44	OPTIONAL. 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 the associated IDN Table with variants 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 3454, 3490, 3491, and 3743 as well as the ICANN IDN Guidelines at http://www.icann.org/en/topics/idn/implementation-guidelines.htm.	IDNs are an optional service at time of launch. Absence of IDN implementation or plans will not detract from an applicant's score. Applicants who respond to this question with plans for implementation of IDNs at time of launch will be scored according to the criteria indicated here.	0-2	IDNs are an optional service. Complete answer demonstrates: (1) complete knowledge and understanding of this aspect of registry technical requirements; (2) a technical plan that is adequately resourced in the planned costs detailed in the financial section; (3) consistency with the commitments made to registrants in the purpose of the registration and registry services descriptions; and (4) issues regarding use of scripts are settled and IDN tables are complete and publicly available.	2 - exceeds requirements: Response includes (1) Evidence of highly developed and detailed procedures for IDNs, including complete IDN tables, compliance with IDNA/IDN guidelines and RFCs, periodic monitoring of IDN operations; (2) Evidence of ability to resolve rendering and known IDN issues or IDN spoofing attacks; (3) Full interplay and consistency of technical and business requirements; and (4) Evidence of technical resources are already on hand or committed. 1 - meets requirements: Response includes (1) Adequate level of detail to substantially demonstrate capability and knowledge required to meet this element; (2) Evidence of adequate implementation plans for IDNs in compliance with IDN/IDNA guidelines; (3) IDN plans are consistent with the overall business approach as described in the application; (4) Demonstrates that technical resources required to carry through the plans for this element are readily available. 0 - fails requirements: Does not meet the requirements to score a 1.
Demonstration of Financial Capability	45	Financial Statements: provide audited or certified financial statements for the most recently completed fiscal year for the applicant, and unaudited financial statements for the most recently ended interim financial period for the applicant. For newly-formed applicants, provide the latest available financial statements. Financial statements are used in the analysis of projections and costs. (Responses to this question will be kept confidential.)	The questions in this section (45-50) are intended to give applicants an opportunity to demonstrate their financial capabilities to run a registry.	0-1	Audited or certified financial statements are prepared in accordance with IFRS (International Financial Reporting Standards) adopted by the IASB (International Accounting Standards Board) or U.S. GAAP (Generally Accepted Accounting Principles). This will include a balance sheet and income statement reflecting the applicant's financial position and results of operations. In the event the applicant is a newly formed entity for the purposes of applying for a gTLD and without an operating history, the applicant must submit pro forma financial statements reflecting the entity's projected capitalization for the registry operator. Funding in this latter case must be verifiable as a true and accurate reflection and cannot include prospective funding. Where audited or certified statements are not available, applicant has provided adequate explanation as to practices in its jurisdiction and has provided, at a minimum, unaudited financial statements.	1 - meets requirements: Complete audited or certified financial statements are provided, at the highest level available in the applicant's jurisdiction. Where such financial statements are not available, the applicant has provided an explanation and has provided, at a minimum, unaudited financial statements. 0 - fails requirements: Does not meet the requirements to score 1. For example, entity with an operating history fails to provide audited or certified statements.
	46	Projections Template: provide financial projections for costs and funding using Template 1 (attached) for the most likely scenario. The template is intended to provide commonality among TLD applications and thereby facilitate the evaluation process. Include explanations for any significant variances between years (or expected in years beyond the timeframe of the template) in any category of costing or funding. Describe the basis for the numbers provided, including studies, reference data, or other steps taken to develop the responses and validate any assumptions made. (Responses to this question will be kept confidential.)		0-2	Applicant has provided a thorough model that demonstrates a sustainable business (even if break-even is not achieved through the first three years of operation). Applicant's description of projections development is sufficient to show due diligence and basis for projections.	2 - exceeds requirements: (1) Model is described in sufficient detail to be determined as a conservative balance of cost, funding and risk, i.e., funding and costs are highly consistent and are representative of a robust on-going concern; (2) Anticipated ranges in revenue and cost are explained in detail. All operations are funded even at negative ends of expected ranges; and (3) Lead-up work done in developing projections is described fully and indicates a sound basis for numbers provided. 1 - meets requirements: (1) Demonstrates resources and plan for sustainable operations; (2) Most important, financial assumptions about the registry services, funding and market are identified; (3) Financial estimates are defensible; and (4) Model is described in sufficient detail to be determined as a reasonable balance of cost, funding and risk, i.e., funding and costs are consistent and are representative of an on-going concern. 0 - fails requirements: Does not meet the requirements to score a 1.

	#	Question	Notes	Scoring Range	Criteria	Scoring
	47	(a) Costs: describe and explain the expected costs of setting up and operating the proposed Registry. As described in the Applicant Guidebook, the information provided will be considered in light of the entire application and the evaluation criteria. Therefore, this answer should agree with the information provided in the template to: 1) maintain registry operations, 2) provide registry services described above, and 3) satisfy the technical requirements described in the Demonstration of Technical & Operational Capability section. **(Responses to this question will be kept confidential.)**		0-2	Costs identified are consistent with the proposed registry services, adequately fund technical requirements, and are consistent with proposed mission/purpose of the registry. A reasonable person with registry technical operations experience would agree the costs projected are reasonable for a registry of size and scope described in the application. Costs identified include the financial instrument described in question 50 below.	**2 - exceeds requirements**: (1) Cost elements described are clearly and separately tied to each of the aspects of registry operations: registry services, technical requirements, and other aspects as described by the applicant; (2) Estimated costs are conservative and consistent with an operation of the registry volume/scope/size as described by the applicant; (3) Most estimates are derived from actual examples of previous registry operations or equivalent; and (4) Conservative estimates are based on those experiences and describe a range of anticipated costs and use the high end of those estimates. **1 - meets requirements:** (1) Cost elements described reasonably cover all of the aspects of registry operations: registry services, technical requirements and other aspects as described by the applicant; and (2) Estimated costs are consistent and defensible with an operation of the registry volume/scope/size as described by the applicant. **0 - fails requirements:** Does not meet the requirements to score a 1.
		(b) Describe anticipated ranges in projected costs. Describe factors that affect those ranges. **(Responses to this question will be kept confidential.)**				
	48	(a) Funding and Revenue: Funding can be derived from several sources (e.g., existing capital or proceeds/revenue from operation of the proposed registry). For each source (as applicable), describe: I) How existing funds will provide resources for both: 1) start-up of operations, and 2) ongoing operations, II) a description of the revenue model including projections for transaction volumes (if the applicant does not intend to rely on registration revenue in order to cover the costs of the registry's operation, it must clarify how the funding for the operation will be developed and maintained in a stable and sustainable manner), III) outside sources of funding, the applicant must (where applicable) provide evidence of the commitment by the party committing the funds. **(Responses to this question will be kept confidential.)**		0-2	Funding resources are clearly identified and adequately provide for registry cost projections. Sources of capital funding are clearly identified, held apart from other potential uses of those funds and available. The plan for transition of funding sources from available capital to revenue from operations (if applicable) is described. Outside sources of funding are documented and verified and must not include prospective sources of funds. Sources of capital funding required to sustain registry operations on an on-going basis are identified. The projected revenues are consistent with the size and projected penetration of the target markets.	**2 - exceeds requirements**: (1) Existing funds are quantified, segregated and earmarked for registry operations; (2) If on-going operations are to be resourced from existing funds (rather than revenue from on-going operations) that funding is segregated and earmarked for this purpose only in an amount adequate for three years operation; (3) Revenues are clearly tied to projected business volumes, market size and penetration; and (4) Assumptions made are regarded as conservative by industry experts. **1 - meets requirements:** (1) Existing funds are quantified, identified as available and budgeted; (2) If on-going operations are to be resourced from existing funds (rather than revenue from on-going operations) that funding is quantified and its sources identified in an amount adequate for three years operation; (3) Revenues are directly related to projected business volumes, market size and penetration; and (4) Assumptions made are regarded as reasonable by industry expert. **0 - fails requirements:** Does not meet the requirements to score a 1.
		(b) Describe anticipated ranges in projected funding and revenue. Describe factors that affect those ranges. **(Responses to this question will be kept confidential.)**				
	49	(a) Contingency Planning: describe your contingency planning: identify any projected barriers to implementation of your business plan and how they affect cost, funding or timeline in your planning, e.g., have you identified any particular regulation, law or policy that might impact the Registry Services offering? **(Responses to this question will be kept confidential.)**		0-2	Contingencies and risks are identified and included in the cost and funding analyses. Action plans are identified in the event contingencies occur. The model is resilient in the event those contingencies occur. Responses address the probability and resource impact of the contingencies identified.	**2 - exceeds requirements** (1) Model identifies thoroughly the key risks and the chances that each will occur: operational, business, legal, and other outside risks; and (2) Action plans and operations adequately resourced in the existing funding and revenue plan even if contingencies occur. **1 - meets requirements:** (1) Model identifies the key risks with sufficient detail to be understood by a business person with experience in this area; (2) Response gives consideration to probability of contingencies identified; and (3) If resources are not available to fund contingencies in the existing plan, funding sources and a plan for obtaining them are identified. **0 - fails requirements:** Does not meet the requirements to score a 1.

16

#	Question	Notes	Scoring Range	Criteria	Scoring
	(b) Describe your contingency planning where funding sources so significantly under run your business plan that material deviations from your implementation model are required. In particular, how will on-going technical requirements be met? Complete a financial projections template (Template 2) for the worst case scenario. **(Responses to this question will be kept confidential.)**				
	(c) Describe your contingency planning where activity volumes so significantly exceed the high projections that material deviation from your implementation model are required. In particular, how will on-going technical requirements be met? **(Responses to this question will be kept confidential.)**				
50	(a) Continuity: Provide a cost estimate for funding basic registry operations on an annual basis. The basic functions of a registry which must be supported even if an applicant's business and/or funding fails are: i) Maintenance of TLD nameservers and DNS for registered domain names; ii) Operation of the Shared Registration System; iii) Provision of Whois service; iv) Maintenance of registrar billing and accounting processes; v) Maintenance of data security processes and regular escrow deposits; vi) Maintenance of IDN Tables (if IDNs are offered); and vii) Provision of DNSSEC in accordance with technical requirements, including storage of key information. List the estimated annual cost for each of these functions (specify currency used).	Registrant protection is critical and thus new gTLD applicants are requested to provide evidence indicating that critical functions will continue to be performed even if the registry fails. Registrant needs are best protected by a clear demonstration the basic registry functions are sustained for an extended period even in the face of registry failure. Therefore, this section is weighted heavily as a clear, objective measure to protect and serve registrants. The applicant has two tasks associated with adequately making this demonstration of continuity for basic registry functions. First, costs for maintaining critical registrant protection functions are to be estimated (Part a). In evaluating the application, the evaluators will adjudge whether the estimate is reasonable given the systems architecture and overall business approach described elsewhere in the application. Second (Part b), methods of securing the funds required to perform those functions for three to five years following the termination of the registry agreement are to be described by the applicant in accordance with the criteria below. Two types of instruments will fulfill this requirement. The applicant must identify which of the two methods is being described. The instrument is required to be in place at the time of the execution of the registry agreement.	0-2	Figures provided are based on an accurate estimate of costs. Documented evidence or detailed plan for ability to fund ongoing basic registry operations for registrants for a period of three to five years in the event of registry failure, default, or until a successor operator can be designated. Evidence of financial wherewithal to fund this requirement prior to delegation. This requirement must be met prior to or concurrent with the execution of the registry agreement.	**3 - exceeds requirements:** (1) Costs are commensurate with technical plans and overall business approach as described in the application; and (2) Financial instrument is secured and in place to provide for on-going operations for at least three years in the event of failure. **1 - meets requirements:** (1) Costs are commensurate with technical plans and overall business approach as described in the application; and (2) Funding is identified and instrument is described to provide for on-going operations of at least three years in the event of failure. **0 - fails requirements:** Does not meet the requirements to score a 1.
	(b) Applicants must provide evidence as to how the funds required for performing these basic registry functions will be available and guaranteed to fund registry operations (for the protection of registrants in the new gTLD) for a minimum of three years following the termination of the registry agreement. ICANN has identified two methods to fulfill this requirement: i) <u>Irrevocable standby letter of credit (LOC)</u> issued by a reputable financial institution. • The amount of the LOC must be equal to or greater than the amount required to fund the basic registry operations specified above for at least three years following the termination of the registry agreement. In the event of a draw upon the letter of credit, the actual payout would be tied to the cost of running those functions. • The LOC must name ICANN or its designee as the beneficiary. Any funds paid out would be provided to the designee who is operating the required registry functions. • The LOC must have a term of at least five years from the delegation of the TLD. The LOC may be structured with an annual expiration date if it contains an evergreen provision providing for annual extensions, without amendment, for an indefinite number of periods until the issuing bank informs the beneficiary of its final expiration or until the beneficiary releases the LOC as evidenced in writing. If the expiration date occurs prior to the fifth anniversary of the delegation of the TLD, applicant will be required to obtain a replacement instrument. • The LOC must be issued by a reputable financial institution insured at the highest level in its jurisdiction. This may include a bank or insurance company with a strong international reputation that has a strong credit rating issued by a third party rating agency such as Standard & Poor's (AA or above), Moody's (Aa or above), or A.M. Best (A-X or above). • The LOC will provide that ICANN or its designee shall be unconditionally entitled to a release of funds (full or partial) thereunder upon delivery of written notice by ICANN or its designee of the termination of the registry agreement for the TLD. • Applicant should attach an original copy of the executed letter of credit or a draft of the				

	#	Question	Notes	Scoring Range	Criteria	Scoring
		letter of credit containing the full terms and conditions. If not yet executed, the Applicant will be required to provide ICANN with an original copy of the executed LOC prior to or concurrent with the execution of the registry agreement. • The LOC must contain at least the following required elements: o Issuing bank and date of issue. o Beneficiary: ICANN / 4676 Admiralty Way, Suite 330 / Marina del Rey, CA 90292 / US, or its designee. o Applicant's complete name and address. o LOC identifying number. o Exact amount in USD. o Expiry date. o Address, procedure, and required forms whereby presentation for payment is to be made. o Conditions: • Partial drawings from the letter of credit may be made provided that such payment shall reduce the amount under the standby letter of credit. • All payments must be marked with the issuing bank name and the bank's standby letter of credit number. • LOC may not be modified, amended, or amplified by reference to any other document, agreement, or instrument. • The LOC is subject to the International Standby Practices (ISP 98) International Chamber of Commerce (Publication No. 590). ii) A deposit into an irrevocable cash escrow account held by a reputable financial institution. • The amount of the deposit must be equal to or greater than the amount required to fund registry operations for at least three years. • Cash is to be held by a third party financial institution which will not allow the funds to be commingled with the Applicant's operating funds or other funds and may only be accessed by ICANN or its designee if certain conditions are met. • The account must be held by a reputable financial institution insured at the highest level in its jurisdiction. This may include a bank or insurance company with a strong international reputation that has a strong credit rating issued by a third party rating agency such as Standard & Poor's (AA or above), Moody's (Aa or above), or A.M. Best (A-X or above). • The escrow agreement relating to the escrow account will provide that ICANN or its designee shall be unconditionally entitled to a release of funds (full or partial) thereunder upon delivery of written notice by ICANN or its designee of the termination of the registry agreement for the TLD. • The escrow agreement must have a term of five years from the delegation of the TLD. • The funds in the deposit escrow account are not considered to be an asset of ICANN. • Any interest earnings less bank fees are to accrue to the deposit, and will be paid back to the applicant upon liquidation of the account to the extent not used to pay the costs and expenses of maintaining the escrow. • The deposit plus accrued interest, less any bank fees in respect of the escrow, is to be returned to the applicant if the funds are not used to fund registry operations due to a triggering event or after five years, whichever is greater. • The Applicant will be required to provide ICANN an explanation as to the amount of the deposit, the institution that will hold the deposit, and the escrow agreement for the account at the time of submitting an application. • Applicant should attach evidence of deposited funds in the escrow account, or evidence of provisional arrangement for deposit of funds. Evidence of deposited funds and terms of escrow agreement must be provided to ICANN prior to or concurrent with the execution of the registry agreement.				

TLD Applicant -- Financial Projections : Instructions

	Start-up Costs	Year 1	Year 2	Year 3	Comments / Notes
Revenue					
(A) Forecasted registration	-	62,000	80,600	104,780	
(B) Registration fee	$ -	$ 5.00	$ 6.00	$ 7.00	
(A*B) Registration revenue	-	310,000	483,600	733,460	
Other revenue / funding	-	35,000	48,000	62,000	
Total Revenue	-	345,000	531,600	795,460	

Cost					
Labor:					
Marketing Labor	25,000	66,000	72,000	81,000	
Customer Support Labor	5,000	68,000	71,000	74,000	
Technical Labor	32,000	45,000	47,000	49,000	
Marketing	40,000	44,000	26,400	31,680	
Facilities	7,000	10,000	12,000	14,400	
General & Administrative	14,000	112,000	122,500	136,000	
Interest and Taxes	2,500	4,000	4,800	5,760	
Equipment	1,800	2,400	2,880	3,456	
Other Costs	12,200	18,000	21,600	25,920	
Total Costs	139,500	369,400	380,180	421,216	

Net Operation (Revenues less Costs)	(139,500)	(24,400)	151,420	374,244	

Capital Expenditures					
Hardware	98,000	21,000	16,000	58,000	
Software	32,000	18,000	24,000	11,000	
Furniture & Equipment	43,000	22,000	14,000	16,000	
	173,000	61,000	54,000	85,000	
Cash Requirements	(312,500)	(85,400)	97,420	289,244	

General Comments (Notes Regarding Assumptions Used, Significant Variances Between Years, etc.):

Comments regarding how the Applicant plans to Fund operations:

General Comments regarding contingencies:

Template 1: Financial Projections: Most Likely Scenario

	Start-up Costs	Year 1	Year 2	Year 3	Comments / Notes
Revenue					
(A) Forecasted registration					
(B) Registration fee					
(A*B) Registration revenue	-	-	-	-	
Other revenue / funding					
Total Revenue	-	-	-	-	
Cost					
Labor:					
Marketing Labor					
Customer Support Labor					
Technical Labor					
Marketing					
Facilities					
General & Administrative					
Interest and Taxes					
Equipment					
Other Costs					
Total Costs	-	-	-	-	
Net Operation (Revenues less Costs)	-	-	-	-	
Capital Expenditures					
Hardware					
Software					
Furniture & Equipment					
	-	-	-	-	
Cash Requirements	-	-	-	-	

General Comments (Notes Regarding Assumptions Used, Significant Variances Between Years, etc.):

Comments regarding how the Applicant plans to Fund operations:

General Comments regarding contingencies:

20

Template 2: Financial Projections: Worst Case Scenario

	Start-up Costs	Year 1	Year 2	Year 3	Comments / Notes
Revenue					
(A) Forecasted registration					
(B) Registration fee					
(A*B) Registration revenue	-	-	-	-	
Other revenue / funding					
Total Revenue	-	-	-	-	
Cost					
Labor:					
Marketing Labor					
Customer Support Labor					
Technical Labor					
Marketing					
Facilities					
General & Administrative					
Interest and Taxes					
Equipment					
Other Costs					
Total Costs	-	-	-	-	
Net Operation (Revenues less Costs)	-	-	-	-	
Capital Expenditures					
Hardware					
Software					
Furniture & Equipment					
	-	-	-	-	
Cash Requirements	-	-	-	-	

General Comments (Notes Regarding Assumptions Used, Significant Variances Between Years, etc.):

Comments regarding how the Applicant plans to Fund operations:

General Comments regarding contingencies:

TLD Applicant -- Financial Projections : Sample

	Start-up Costs	Year 1	Year 2	Year 3	Comments / Notes
Revenue					
(A) Forecasted registration	-	62,000	80,600	104,780	Registration was forecasted based on recent market surveys.
(B) Registration fee	$ -	$ 5.00	$ 6.00	$ 7.00	We do not anticipate significant increases in Registration Fees subsequent to year 3 .
(A*B) Registration revenue	-	310,000	483,600	733,460	
Other revenue / funding	-	35,000	48,000	62,000	Other revenues represent Advertising Revenue from display ads on our website.
Total Revenue	-	345,000	531,600	795,460	
Cost					
Labor:					
Marketing Labor	25,000	66,000	72,000	81,000	
Customer Support Labor	5,000	68,000	71,000	74,000	
Technical Labor	32,000	45,000	47,000	49,000	
Marketing	40,000	44,000	26,400	31,680	
Facilities	7,000	10,000	12,000	14,400	
General & Administrative	14,000	112,000	122,500	136,000	
Interest and Taxes	2,500	4,000	4,800	5,760	
Equipment	1,800	2,400	2,880	3,456	
Other Costs	12,200	18,000	21,600	25,920	
Total Costs	139,500	369,400	380,180	421,216	
Net Operation (Revenues less Costs)	(139,500)	(24,400)	151,420	374,244	
Capital Expenditures					Assumption is that Computer Equipment has a three year useful life and then must be replaced.
Hardware	98,000	21,000	16,000	58,000	
Software	32,000	18,000	24,000	11,000	
Furniture & Equipment	43,000	22,000	14,000	16,000	
	173,000	61,000	54,000	85,000	
Cash Requirements	(312,500)	(85,400)	97,420	289,244	

General Comments (Notes Regarding Assumptions Used, Significant Variances Between Years, etc.):
We expect the number of registrations to grow at approximately 30% per year with an increase in the registration fee of $1 per year for the first three years. We anticipate our costs will increase at a controlled pace over the first three years except for Marketing costs which will be higher in the start-up and first year as we establish our brand name and work to increase registrations. Our capital expenditures will be greatest in the start-up phase and then our need to invest in computer hardware and software will level off after the start-up period. Our investment in Furniture and Equipment will be greatest in the start-up period as be build our infrastructure and then decrease in the following periods.

Comments regarding how the Applicant plans to Fund operations:
We have recently negotiated a line of credit with XYZ Bank (a copy of the fully executed line of credit agreement has been included with our application) and this funding will allow us to purchase necessary Equipment and pay for employees and other Operating Costs during our start-up period and the first few years of operations. We expect that our business model will be self funded (i.e., revenue from operations will cover all anticipated costs and capital expenditures) by the second half of our second year in operation; we also expect to become profitable with positive cash flow in year three.

General Comments regarding contingencies:
Although we expect to be cash flow positive by the end of year 2, the recently negotiated line of credit will cover our operating costs for the first 4 years of operation if necessary. We have also entered into an agreement with XYZ Co. to assume our registrants should our business model not have the ability to sustain itself in future years. Agreement with XYZ Co. has been included with our application.

Draft Applicant Guidebook, v3

Module 3

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.

2 October 2009

Module 3

Dispute Resolution Procedures

This module describes the purpose of the objection and dispute resolution mechanisms, the grounds for lodging a formal objection to a gTLD application, the general procedures for filing or responding to an objection, and the manner in which dispute resolution proceedings are conducted.

This module also discusses the guiding principles, or standards, that each dispute resolution panel will apply in reaching its expert determination.

All applicants should be aware of the possibility that an objection may be filed against any application, and of the procedures and options available in the event of such an objection.

3.1   Purpose and Overview of the Dispute Resolution Process

The independent dispute resolution process is designed to protect certain limited interests and rights. The process provides a path for formal objections during evaluation of the applications. It allows a party with standing to have its objection considered before a panel of qualified experts.

A formal objection can be filed only on four enumerated grounds, as described in this module. A formal objection initiates a dispute resolution proceeding. In filing an application for a gTLD, the applicant agrees to accept the applicability of this gTLD dispute resolution process. Similarly, an objector accepts the applicability of this gTLD dispute resolution process by filing its objection.

3.1.1   Grounds for Objection

An objection may be filed on any one of the following four grounds:

String Confusion Objection – The applied-for gTLD string is confusingly similar to an existing TLD or to another applied-for gTLD string in the same round of applications.

Legal Rights Objection – The applied-for gTLD string infringes the existing legal rights of the objector.

Morality and Public Order Objection – The applied-for gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under international principles of law.

Community Objection – There is substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.

The rationales for these objection grounds are discussed in the final report of the ICANN policy development process for new gTLDs. For more information on this process, see http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm.

3.1.2   Standing to Object

Objectors must satisfy standing requirements to have their objections considered. As part of the dispute proceedings, all objections will be reviewed by a panel of experts designated by the applicable Dispute Resolution Service Provider (DRSP) to determine whether the objector has standing to object. Standing requirements for the four objection grounds are:

Objection ground	Who may object
String confusion	Existing TLD operator or gTLD applicant in current round
Legal rights	Rightsholders
Morality and Public Order	No limitations on who may file – however, subject to a "quick look" designed for early conclusion of frivolous objections
Community	Established institution

3.1.2.1   String Confusion Objection

Two types of entities have standing to object:

- An existing TLD operator may file a string confusion objection to assert string confusion between an applied-for gTLD and the TLD that it currently operates.

- Any gTLD applicant in this application round may file a string confusion objection to assert string confusion between an applied-for gTLD and the gTLD for which it has applied, where string confusion between the two applicants has not already been found. That is, an applicant does not

3-2

have standing to object to another application with which it is already in a contention set.

In the case where an existing TLD operator successfully asserts string confusion with an applicant, the application will be rejected.

In the case where a gTLD applicant successfully asserts string confusion with another applicant, the only possible outcome is for both applicants to be placed in a contention set and to be referred to a contention resolution procedure (refer to Module 4, String Contention Procedures). If an objection by one gTLD applicant to another gTLD applicant is unsuccessful, the applicants may both move forward in the process without being considered in contention with one another.

3.1.2.2   *Legal Rights Objection*

Only a rightsholder has standing to file a legal rights objection. The source and documentation of the existing legal rights the objector is claiming (which may include either registered or unregistered marks) are infringed by the applied-for gTLD must be included in the filing.

3.1.2.3   *Morality and Public Order Objection*

Anyone may file a Morality and Public Order Objection. Due to the inclusive standing base, however, objectors are subject to a "quick look" procedure designed to identify and eliminate frivolous and/or abusive objections. An objection found to be manifestly unfounded and/or an abuse of the right to object may be dismissed at any time.

3.1.2.4   *Community Objection*

Established institutions associated with clearly delineated communities are eligible to file a community objection. The community named by the objector must be a community strongly associated with the applied-for gTLD string in the application that is the subject of the objection. To qualify for standing for a community objection, the objector must prove both of the following:

It is an established institution – Factors that may be considered in making this determination include:

- Level of global recognition of the institution;

- Length of time the institution has been in existence; and

- Public historical evidence of its existence, such as the presence of formal charter or national or

international registration, or validation by a government, inter-governmental organization, or treaty. The institution must not have been established solely in conjunction with the gTLD application process.

It has an ongoing relationship with a clearly delineated community – Factors that may be considered in making this determination include:

- The presence of mechanisms for participation in activities, membership, and leadership;

- Institutional purpose related to the benefit of the associated community;

- Performance of regular activities that benefit the associated community; and

- The level of formal boundaries around the community.

The panel will perform a balancing of the factors listed above in making its determination. It is not expected that an objector must demonstrate satisfaction of each and every factor considered in order to satisfy the standing requirements.

3.1.3 Dispute Resolution Service Providers

To trigger a dispute resolution proceeding, an objection must be filed by the posted deadline date, directly with the appropriate DRSP for each objection ground.

- The International Centre for Dispute Resolution has agreed in principle to administer disputes brought pursuant to string confusion objections.

- The Arbitration and Mediation Center of the World Intellectual Property Organization has agreed in principle to administer disputes brought pursuant to legal rights objections.

- The International Center of Expertise of the International Chamber of Commerce has agreed in principle to administer disputes brought pursuant to Morality and Public Order and Community Objections.

ICANN selected DRSPs on the basis of their relevant experience and expertise, as well as their willingness and ability to administer dispute proceedings in the new gTLD Program. The selection process began with a public call for

expressions of interest[1] followed by dialogue with those candidates who responded. The call for expressions of interest specified several criteria for providers, including established services, subject matter expertise, global capacity, and operational capabilities. An important aspect of the selection process was the ability to recruit panelists who will engender the respect of the parties to the dispute.

3.1.4   Options in the Event of Objection

Applicants whose applications are the subject of an objection have the following options:

The applicant can work to reach a settlement with the objector, resulting in withdrawal of the objection or the application;

The applicant can file a response to the objection and enter the dispute resolution process (refer to Section 3.2); or

The applicant can withdraw, in which case the objector will prevail by default and the application will not proceed further.

If for any reason the applicant does not file a response to an objection, the objector will prevail by default.

3.1.5   Independent Objector

A formal objection to a gTLD application may also be filed by the Independent Objector (IO). The IO does not act on behalf of any particular persons or entities, but acts solely in the best interests of the public who use the global Internet.

In light of this public interest goal, the Independent Objector is limited to filing objections on the grounds of Morality and Public Order and Community.

Neither ICANN staff nor the ICANN Board of Directors has authority to direct or require the IO to file or not file any particular objection. If the IO determines that an objection should be filed, he or she will initiate and prosecute the objection in the public interest.

Mandate and Scope—The IO may file objections against "highly objectionable" gTLD applications to which no objection has been filed. The IO is limited to filing two types of objections: (1) Morality and Public Order objections and

---

[1] *See* http://www.icann.org/en/announcements/announcement-21dec07.htm.

(2) Community objections. The IO is granted standing to file objections on these enumerated grounds, notwithstanding the regular standing requirements for such objections (see subsection 3.1.2).

The IO may file a Morality and Public Order objection against an application even if a Community objection has been filed, and vice versa.

The IO may file an objection against an application, notwithstanding the fact that a String Confusion objection or a Legal Rights objection was filed.

Absent extraordinary circumstances, the IO is not permitted to file an objection to an application where an objection has already been filed on the same ground.

The IO may consider public comment when making an independent assessment whether an objection is warranted. ICANN will submit comments to the IO from the appropriate time period, running through the Initial Evaluation period until the close of the deadline for the IO to submit an objection.

Selection – The IO will be selected by ICANN, through an open and transparent process, and retained as an independent consultant. The Independent Objector will be an individual with considerable experience and respect in the Internet community, unaffiliated with any gTLD applicant.

Although recommendations for IO candidates from the community are welcomed, the IO must be and remain independent and unaffiliated with any of the gTLD applicants. The various rules of ethics for judges and international arbitrators provide models for the IO to declare and maintain his/her independence.

The IO's (renewable) tenure is limited to the time necessary to carry out his/her duties in connection with a single round of gTLD applications.

Budget and Funding – The IO's budget would comprise two principal elements: (a) salaries and operating expenses, and (b) dispute resolution procedure costs – both of which should be funded from the proceeds of new gTLD applications.

As an objector in dispute resolution proceedings, the IO is required to pay filing and administrative fee, including panel fees, just as all other objectors are required to do.

Those payments will be refunded by the DRSP in cases where the IO is the prevailing party.

In addition, the IO will incur various expenses in presenting objections before DRSP panels that will not be reimbursed, regardless of the outcome. These expenses include the fees and expenses of outside counsel (if retained) and the costs of legal research or factual investigations.

3.2   Filing Procedures

The information included in this section provides a summary of procedures for filing:

- Objections; and

- Responses to objections.

For a comprehensive statement of filing requirements applicable generally, refer to the New gTLD Dispute Resolution Procedure ("Procedure") included as an attachment to this module. In the event of any discrepancy between the information presented in this module and the Procedure, the Procedure shall prevail.

Note that the rules and procedures of each DRSP specific to each objection ground must also be followed.

- For a String Confusion Objection, the applicable DRSP Rules are the ICDR Supplementary Procedures for ICANN's New gTLD Program. These rules are under development and should be available shortly.

- For a Legal Rights Objection, the applicable DRSP Rules are the WIPO Rules for New gTLD Dispute Resolution. These rules are available in draft form and have been posted along with this module.

- For a Morality and Public Order Objection, the applicable DRSP Rules are the Rules for Expertise of the International Chamber of Commerce.

- For a Community Objection, Objection, the applicable DRSP Rules are the Rules for Expertise of the International Chamber of Commerce.

3.2.1   Objection Filing Procedures

The procedures outlined in this subsection must be followed by any party wishing to file a formal objection to an application that has been posted by ICANN. Should an

applicant wish to file a formal objection to another gTLD application, it would follow these same procedures.

- All objections must be filed electronically with the appropriate DRSP by the posted deadline date. Objections will not be accepted by the DRSPs after this date.

- All objections must be filed in English.

- Each objection must be filed separately. An objector wishing to object to several applications must file a separate objection and pay the accompanying filing fees for each application that is the subject of an objection. If an objector wishes to object to an application on more than one ground, the objector must file separate objections and pay the accompanying filing fees for each objection ground.

Each objection filed by an objector must include:

- The name and contact information of the objector.

- A statement of the objector's basis for standing; that is, why the objector believes it has the right to object.

- A description of the basis for the objection, including:

  - A statement giving the specific ground upon which the objection is being filed.

  - A detailed explanation of the validity of the objection and why it should be upheld.

- Copies of any documents that the objector considers to be a basis for the objection.

Objections are limited to 5000 words or 20 pages, whichever is less, excluding attachments.

An objector must provide copies of all submissions to the DRSP associated with the objection proceedings to the applicant, and to ICANN (except that confidential communications between the DRSP and objector shall not be provided to ICANN).

ICANN and/or the DRSPs will publish, and regularly update, a list on its website identifying all objections as they are filed and ICANN is notified.

3.2.2   *Objection Filing Fees*

At the time an objection is filed, the objector is required to pay a nonrefundable filing fee in the amount set and published by the relevant DRSP. If the filing fee is not paid, the DRSP will dismiss the objection without prejudice. See Section 1.5 of Module 1 regarding fees.

3.2.3   *Response Filing Procedures*

Upon notification that ICANN has published the list of all objections filed (refer to subsection 3.2.1), the DRSPs will notify the parties that responses must be filed within 30 calendar days of receipt of that notice. DRSPs will not accept late responses. Any applicant that fails to respond to an objection within the 30-day response period will be in default, which will result in the objector prevailing.

- All responses must be filed in English.

- Each response must be filed separately. That is, an applicant responding to several objections must file a separate response and pay the accompanying filing fee to respond to each objection.

- Responses must be filed electronically.

Each response filed by an applicant must include:

- the name and contact information of the applicant.

- a point-by-point response to the claims made by the objector.

- any copies of documents that it considers to be a basis for the response.

 Responses are limited to 5000 words or 20 pages, whichever is less, excluding attachments.

Each applicant must provide copies of all submissions to the DRSP associated with the objection proceedings to the objector and to ICANN (except that confidential communications between the DRSP and responder shall not be provided to ICANN).

3.2.4   *Response Filing Fees*

At the time an applicant files its response, it is required to pay a nonrefundable filing fee in the amount set and published by the relevant DRSP, which will be the same as

the filing fee paid by the objector. If the filing fee is not paid, the response will be disregarded.

3.3   Objection Processing Overview

The information below provides an overview of the process by which DRSPs administer dispute proceedings that have been initiated. For comprehensive information, please refer to the New gTLD Dispute Resolution Procedure (included as an attachment to this module).

3.3.1   Administrative Review

Each DRSP will conduct an administrative review of each objection for compliance with all procedural rules within 14 calendar days of receiving the objection. Depending on the number of objections received, the DRSP may ask ICANN for a short extension of this deadline.

If the DRSP finds that the objection complies with procedural rules, the objection will be deemed filed, and the proceedings will continue. If the DRSP finds that the objection does not comply with procedural rules, the DRSP will dismiss the objection and close the proceedings without prejudice to the objector's right to submit a new objection that complies with procedural rules. The DRSP's review or rejection of the objection will not interrupt the time limit for filing an objection.

3.3.2   Consolidation of Objections

Once the DRSP receives and processes all objections, at its discretion the DRSP may elect to consolidate certain objections. The DRSP shall endeavor to decide upon consolidation prior to issuing its notice to applicants that the response should be filed and, where appropriate, shall inform the parties of the consolidation in that notice.

An example of a circumstance in which consolidation might occur is multiple objections to the same application based on the same ground.

In assessing whether to consolidate objections, the DRSP will weigh the efficiencies in time, money, effort, and consistency that may be gained by consolidation against the prejudice or inconvenience consolidation may cause. The DRSPs will endeavor to have all objections resolved on a similar timeline. It is intended that no sequencing of objections will be established.

New gTLD applicants and objectors also will be permitted to propose consolidation of objections, but it will be at the DRSP's discretion whether to agree to the proposal.

ICANN continues to strongly encourage all of the DRSPs to consolidate matters whenever practicable.

3.3.3   *Negotiation and Mediation*

The parties to a dispute resolution proceeding are encouraged—but not required—to participate in negotiations and/or mediation aimed at settling the dispute. Each DRSP has experts who can be retained as mediators to facilitate this process, should the parties elect to do so, and the DRSPs will communicate with the parties concerning this option and any associated fees.

If a mediator is appointed, that person may not serve on the panel constituted to issue an expert determination in the related dispute.

There are no automatic extensions of time associated with the conduct of negotiations or mediation. The parties may submit joint requests for extensions of time to the DRSP according to its procedures, and the DRSP or the panel, if appointed, will decide whether to grant the requests, although extensions will be discouraged. Absent exceptional circumstances, the parties must limit their requests for extension to 30 calendar days.

3.3.4   *Selection of Expert Panels*

A panel will consist of appropriately qualified experts appointed to each proceeding by the designated DRSP. Experts must be independent of the parties to a dispute resolution proceeding. Each DRSP will follow its adopted procedures for requiring such independence, including procedures for challenging and replacing an expert for lack of independence.

There will be one expert in proceedings involving a string confusion objection.

There will be one expert, or, if all parties agree, three experts with relevant experience in intellectual property rights disputes in proceedings involving an existing legal rights objection.

There will be three experts recognized as eminent jurists of international reputation, in proceedings involving a morality and public order objection.

There will be one expert in proceedings involving a community objection.

Neither the experts, the DRSP, ICANN, nor their respective employees, directors, or consultants will be liable to any party in any action for damages or injunctive relief for any act or omission in connection with any proceeding under the dispute resolution procedures.

3.3.5   Adjudication

The panel may decide whether the parties shall submit any written statements in addition to the filed objection and response, and may specify time limits for such submissions.

In order to achieve the goal of resolving disputes rapidly and at reasonable cost, procedures for the production of documents shall be limited. In exceptional cases, the panel may require a party to produce additional evidence.

Disputes will usually be resolved without an in-person hearing. The panel may decide to hold such a hearing only in extraordinary circumstances.

3.3.6   Expert Determination

The DRSPs' final expert determinations will be in writing and will include:

- A summary of the dispute and findings;

- An identification of the prevailing party; and

- The reasoning upon which the expert determination is based.

Unless the panel decides otherwise, each DRSP will publish all decisions rendered by its panels in full on its website.

The findings of the panel will be considered an expert determination and advice that ICANN will accept within the dispute resolution process.

3.3.7   Dispute Resolution Costs

Before acceptance of objections, each DRSP will publish a schedule of costs or statement of how costs will be calculated for the proceedings that it administers under this procedure. These costs cover the fees and expenses of the members of the panel and the DRSP's administrative costs.

ICANN expects that string confusion and legal rights objection proceedings will involve a fixed amount charged

by the panelists while morality and public order and community objection proceedings will involve hourly rates charged by the panelists.

Within ten (10) business days of constituting the panel, the DRSP will estimate the total costs and request advance payment in full of its costs from both the objector and the applicant. Each party must make its advance payment within ten (10) days of receiving the DRSP's request for payment and submit to the DRSP evidence of such payment. The respective filing fees paid by the parties will be credited against the amounts due for this advance payment of costs.

The DRSP may revise its estimate of the total costs and request additional advance payments from the parties during the resolution proceedings.

Additional fees may be required in specific circumstances; for example, if the DRSP receives supplemental submissions or elects to hold a hearing.

If an objector fails to pay these costs in advance, the DRSP will dismiss its objection and no fees paid by the objector will be refunded.

If an applicant fails to pay these costs in advance, the DSRP will sustain the objection and no fees paid by the applicant will be refunded.

After the hearing has taken place and the panel renders its expert determination, the DRSP will refund any costs paid in advance to the prevailing party.

3.4   Dispute Resolution Principles (Standards)

Each panel will use appropriate general principles (standards) to evaluate the merits of each objection. The principles for adjudication on each type of objection are specified in the paragraphs that follow. The panel may also refer to other relevant rules of international law in connection with the standards.

The objector bears the burden of proof in each case.

The principles outlined below are subject to evolution based on ongoing consultation with DRSPs, legal experts, and the public.

3.4.1   String Confusion Objection

A DRSP panel hearing a string confusion objection will consider whether the applied-for gTLD string is likely to result in string confusion. String confusion exists where a string so nearly resembles another that it is likely to deceive or cause confusion. For a 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.

3.4.2   Legal Rights Objection

In interpreting and giving meaning to GNSO Recommendation 3 ("Strings must not infringe the existing legal rights of others that are recognized or enforceable under generally accepted and internationally recognized principles of law"), a DRSP panel of experts presiding over a legal rights objection will determine whether the potential use of the applied-for gTLD by the applicant takes unfair advantage of the distinctive character or the reputation of the objector's registered or unregistered trademark or service mark ("mark"), or unjustifiably impairs the distinctive character or the reputation of the objector's mark, or otherwise creates an impermissible likelihood of confusion between the applied-for gTLD and the objector's mark, by considering the following non-exclusive factors:

1. Whether the applied-for gTLD is identical or similar, including in appearance, phonetic sound or meaning, to the objector's existing mark.

2. Whether the objector's acquisition and use of rights in the mark has been bona fide.

3. Whether and to what extent there is recognition in the relevant sector of the public of the sign corresponding to the gTLD, as the mark of the objector, of the applicant or of a third party.

4. Applicant's intent in applying for the gTLD, including whether the applicant, at the time of application for the gTLD, had knowledge of the objector's mark, or could not have reasonably been unaware of that mark, and including whether the applicant has engaged in a pattern of conduct whereby it applied for or operates TLDs or registrations in TLDs which are identical or confusingly similar to the marks of others.

5. Whether and to what extent the applicant has used, or has made demonstrable preparations to use, the sign corresponding to the gTLD in connection with a bona fide offering of goods or services or a bona fide

provision of information in a way that does not interfere with the legitimate exercise by the objector of its mark rights.

6. Whether the applicant has marks or other intellectual property rights in the sign corresponding to the gTLD, and, if so, whether any acquisition of such a right in the sign, and use of the sign, has been bona fide, and whether the purported or likely use of the gTLD by the applicant is consistent with such acquisition or use.

7. Whether and to what extent the applicant has been commonly known by the sign corresponding to the gTLD, and if so, whether any purported or likely use of the gTLD by the applicant is consistent therewith and bona fide.

8. Whether the applicant's intended use of the gTLD would create a likelihood of confusion with the objector's mark as to the source, sponsorship, affiliation, or endorsement of the gTLD.

3.4.3   Morality and Public Order Objection

An expert panel hearing a morality and public order objection will consider whether the applied-for gTLD string is contrary to general principles of international law for morality and public order, as reflected in relevant international agreements. Under these principles, everyone has the right to freedom of expression, but the exercise of this right carries with it special duties and responsibilities. Accordingly, certain limited restrictions may apply.

The grounds upon which an applied-for gTLD string may be considered contrary to morality and public order according to internationally recognized standards are:

- Incitement to or promotion of violent lawless action;

- Incitement to or promotion of discrimination based upon race, color, gender, ethnicity, religion or national origin;

- Incitement to or promotion of child pornography or other sexual abuse of children; or

- A determination that an applied-for gTLD string would be contrary to equally generally accepted identified legal norms relating to morality and public order that are recognized under general principles of international law.

3.4.4 Community Objection

The four tests described here will enable a DRSP panel to determine whether there is substantial opposition from a significant portion of the community to which the string may be targeted. For an objection to be successful, the objector must prove that:

- The community invoked by the objector is a clearly delineated community;

- Community opposition to the application is substantial; and

- There is a strong association between the community invoked and the applied-for gTLD string; and

- There is a likelihood of detriment to the community named by the objector if the gTLD application is approved.

Each of these tests is described in further detail below.

Community – The objector must prove that the community expressing opposition can be regarded as a clearly delineated community. A panel could balance a number of factors to determine this, including:

- The level of public recognition of the group as a community at a local and/or global level;

- The level of formal boundaries around the community and what persons or entities are considered to form the community;

- The length of time the community has been in existence;

- The global distribution of the community (this may not apply if the community is territorial); and

- The number of people or entities that make up the community.

If opposition by a number of people/entities is found, but the group represented by the objector is not determined to be a clearly delineated community, the objection will fail.

Substantial Opposition – The objector must prove substantial opposition within the community it has identified itself as representing. A panel could balance a number of

factors to determine whether there is substantial opposition, including:

- Number of expressions of opposition relative to the composition of the community;

- Level of recognized stature or weight among sources of opposition;

- Distribution or diversity among sources of expressions of opposition, including:

  - Regional

  - Subsectors of community

  - Leadership of community

  - Membership of community

- Historical defense of the community in other contexts; and

- Costs incurred by objector in expressing opposition, including other channels the objector may have used to convey opposition.

If some opposition within the community is determined, but it does not meet the standard of substantial opposition, the objection will fail.

Targeting – The objector must prove a strong association between the applied-for gTLD string and the community represented by the objector. Factors that could be balanced by a panel to determine this include:

- Statements contained in application;

- Other public statements by the applicant;

- Associations by the public.

If opposition by a community is determined, but there is no strong association between the community and the applied-for gTLD string, the objection will fail.

Detriment – The objector must prove that there is a likelihood of detriment to the rights or legitimate interests of its associated community. Factors that could be used by a panel in making this determination include:

- Damage to the reputation of the community that would result from the applicant's operation of the applied-for gTLD string;

- Evidence that the applicant is not acting or does not intend to act in accordance with the interests of the community or of users more widely, including evidence that the applicant has not proposed or does not intend to institute effective security protection for user interests;

- Interference with the core activities of the community that would result from the applicant's operation of the applied-for gTLD string; and

- Dependence of the community on the DNS for its core activities.

If opposition by a community is determined, but there is no likelihood of detriment to the community resulting from the applicant's operation of the applied-for gTLD, the objection will fail.

The objector must meet all four tests in the standard for the objection to prevail.

Defenses to a Community Objection – Satisfaction of the standing requirements for filing a Community Objection (refer to subsection 3.1.2.4) by a community-based applicant is a complete defense to an objection filed on community grounds.

To invoke the complete defense, the community-based applicant must affirmatively prove, in its response to the objection, that it meets all elements of the standing requirements.

A complete defense, based on standing requirements, may not be invoked by a standard applicant whose application is the subject of a Community objection. However, a standard applicant may prevail in the event that a Community objection is filed against it, and the applicant can otherwise present a defense to the objection.

DRAFT - New gTLD Program – Objection and Dispute Resolution

No – 7 Days to Correct

Party with standing files objection directly with Dispute Resolution Service Provider (DRSP) for these grounds:

- *String Confusion*
- *Legal Rights*
- *Morality and Public Order; and/or*
- *Community*

Objector pays filing fee directly to DRSP

Objection filing period opens

An applicant may face anywhere from zero objections to multiple objections in any of the four areas

Objection filed with correct DRSP?

Yes

Objection filing period closes

Administrative Review of objections

DRSP posts objection details on its Web site

ICANN publishes objections announcement

DRSPs notify applicants of relevant objections

30 Days

Applicant files response and pays filing fee

Consolidation of objections, if applicable

If the DRSP itself has not decided to consolidate two or more Objections, any Applicant or Objector may propose the consolidation of Objections. The DRSP shall make a determination whether to consolidate.

30 Days

DRSP appoints panel

10 Days

DRSP sends estimation of costs to parties

10 Days

45 Days

Advance payment of costs due

If payment is not received from:
- The objector, the Objection shall be dismissed
- The applicant, the Objection will have been deemed to be sustained

Expert Determination

Does applicant clear all objections?

No

Applicant withdraws

Yes

Applicant proceeds to subsequent stage

Attachment to Module 3

New gTLD Dispute Resolution Procedure

These Procedures were designed with an eye toward timely and efficient dispute resolution. As part of the New gTLD Program, these Procedures apply to all proceedings administered by each of the dispute resolution service providers (DRSP). Each of the DRSPs has a specific set of rules or will have supplementary procedures that will also apply to such proceedings.

NEW GTLD DISPUTE RESOLUTION PROCEDURE

Article 1.   ICANN's New gTLD Program

(a)   The Internet Corporation for Assigned Names and Numbers ("ICANN") has implemented a program for the introduction of new generic Top-Level Domain Names ("gTLDs") in the internet. There will be a succession of rounds, during which applicants may apply for new gTLDs, in accordance with terms and conditions set by ICANN.

(b)   The new gTLD program includes a dispute resolution procedure, pursuant to which disputes between a person or entity who applies for a new gTLD and a person or entity who objects to that gTLD are resolved in accordance with this New gTLD Dispute Resolution Procedure (the "Procedure").

(c)   Dispute resolution proceedings shall be administered by a Dispute Resolution Service Provider ("DRSP") in accordance with this Procedure and the applicable DRSP Rules that are identified in Article 4(b).

(d)   By applying for a new gTLD, an applicant accepts the applicability of this Procedure and the applicable DRSP's Rules that are identified in Article 4(b); by filing an objection to a new gTLD, an objector accepts the applicability of this Procedure and the applicable DRSP's Rules that are identified in Article 4(b). The parties cannot derogate from this Procedure without the express approval of ICANN and from the applicable DRSP Rules without the express approval the relevant DRSP.

Article 2.   Definitions

(a)   The "Applicant" or "Respondent" is an entity that has applied to ICANN for a new gTLD and that will be the party responding to the Objection.

(b)   The "Objector" is one or more persons or entities who have filed an objection against a new gTLD for which an application has been submitted.

(c)   The "Panel" is the panel of Experts, comprising one or three "Experts", that has been constituted by a DRSP in accordance with this Procedure and the applicable DRSP Rules that are identified in Article 4(b).

(d)   The "Expert Determination" is the decision upon the merits of the Objection that is rendered by a Panel in a proceeding conducted under this Procedure and the applicable DRSP Rules that are identified in Article 4(b).

(e)   The grounds upon which an objection to a new gTLD may be filed are set out in full in [●]. Such grounds are identified in this Procedure, and are based upon the Final Report on the Introduction of New Generic Top-Level Domains, dated 7 August 2007, issued by the ICANN Generic Names Supporting Organization (GNSO), as follows:

(i)   "String Confusion Objection" refers to the objection that the string comprising the potential gTLD is confusingly similar to an existing top-level domain or another string applied for in the round of applications.

(ii)   "Existing Legal Rights Objection" refers to the objection that the string comprising the potential new gTLD infringes the existing legal rights of others that are recognized or enforceable under generally accepted and internationally recognized principles of law.

(iii)   "Morality and Public Order Objection" refers to the objection that the string comprising the potential new gTLD is contrary to generally accepted legal norms relating to morality and public order that are recognized under international principles of law.

(iv)   "Community Objection" refers to the objection that there is substantial opposition to the application from a significant portion of the community to which the string may be explicitly or implicitly targeted.

(f)   "DRSP Rules" are the rules of procedure of a particular DRSP that have been identified as being applicable to objection proceedings under this Procedure.

Article 3.   Dispute Resolution Service Providers

The various categories of disputes shall be administered by the following DRSPs:

(a)   String Confusion Objections shall be administered by the International Centre for Dispute Resolution.

(b)   Existing Legal Rights Objections shall be administered by the Arbitration and Mediation Center of the World Intellectual Property Organization.

(c)   Morality and Public Order Objections shall be administered by the International Centre for Expertise of the International Chamber of Commerce.

(d)   Community Objections shall be administered by the International Centre for Expertise of the International Chamber of Commerce.

Article 4.   Applicable Rules

(a)   All proceedings before the Panel shall be governed by this Procedure and by the DRSP Rules that apply to a particular category of objection. The proceedings shall be deemed an expert determination, and the members of the Panel shall act as experts.

(b)   The applicable DRSP Rules are the following:

(i)   For a String Confusion Objection, the applicable DRSP Rules are the ICDR Supplementary Procedures for ICANN's New gTLD Program.

(ii)   For an Existing Legal Rights Objection, the applicable DRSP Rules are the WIPO Rules for New gTLD Dispute Resolution.

(iii)   For a Morality and Public Order Objection, the applicable DRSP Rules are the Rules for Expertise of the International Chamber of Commerce.

(iv)   For a Community Objection, Objection, the applicable DRSP Rules are the Rules for Expertise of the International Chamber of Commerce.

(c)   In the event of any discrepancy between this Procedure and the applicable DRSP Rules, this Procedure shall prevail.

(d)   The place of the proceedings, if relevant, shall be the location of the DRSP that is administering the proceedings.

(e)   In all cases, the Panel shall ensure that the parties are treated with equality, and that each party is given a reasonable opportunity to present its position.

Article 5.   Language

(a)   The language of all submissions and proceedings under this Procedure shall be English.

(b)   Parties may submit supporting evidence in its original language, provided and subject to the authority of the Panel to determine otherwise, that such evidence is accompanied by an English translation of all relevant text.

Article 6.   Communications and Time Limits

(a)   All communications by the Parties with the DRSPs and Panels must be submitted electronically and copied to ICANN. A Party that wishes to make a submission that is not available in electronic form (e.g., evidentiary models) shall request leave from the Panel to do so, and the Panel, in its sole discretion, shall determine whether to accept the non-electronic submission.

(b)   The DRSP, Panel, Applicant, and Objector shall provide copies to one another and to ICANN of all correspondence (apart from confidential correspondence between the Panel and the DRSP and among the Panel) regarding the proceedings.

(c)   For the purpose of determining the date of commencement of a time limit, a notice or other communication shall be deemed to have been received on the day that it is transmitted in accordance with paragraphs (a) and (b) of this Article.

(d)   For the purpose of determining compliance with a time limit, a notice or other communication shall be deemed to have been sent, made or transmitted if it is dispatched in accordance with paragraphs (a) and (b) of this Article prior to or on the day of the expiration of the time limit.

(e)   For the purpose of calculating a period of time under this Procedure, such period shall begin to run on the day following the day when a notice or other communication is received.

(f)   Unless otherwise stated, all time periods provided in the Procedure are calculated on the basis of calendar days

Article 7.   Filing of the Objection

(a)   A person wishing to object to a new gTLD for which an application has been submitted may file an objection ("Objection"). Any Objection to a proposed new gTLD must be filed within ninety (90) days from ICANN's publication of a report identifying the application for such gTLD.

(b)   The Objection must be filed with the appropriate DRSP, using a model form made available by that DRSP, with copies to ICANN and the Applicant.

(c)   The electronic addresses for filing Objections are the following:

(i)   A String Confusion Objection must be filed at: [●].

(ii)   An Existing Legal Rights Objection must be filed at: [●].

(iii)   A Morality and Public Order Objection must be filed at: [●].

(iv)   A Community Objection must be filed at: [●].

(d)   All Objections must be filed separately:

  (i)   An Objector who wishes to object to an application on more than one ground must file separate objections with the appropriate DRSP(s).

  (ii)   An Objector who wishes to object to more than one gTLD must file separate objections to each gTLD with the appropriate DRSP(s).

(e)   If an Objection is filed with the wrong DRSP, that DRSP shall promptly notify the Objector of the error and shall not process the incorrectly filed Objection. The Objector may then cure the error by filing its Objection with the correct DRSP within seven (7) days of its receipt of the error notice, failing which the Objection shall be disregarded. If the Objection is filed with the correct DRSP within seven (7) days of its receipt of the error notice but after the lapse of the time for submitting an Objection stipulation by Article 7(a) of this Procedure, it shall be deemed to be within this time limit.

Article 8.   Content of the Objection

(a)   The Objection shall contain, *inter alia*, the following information:

  (i)   The names and contact information (address, telephone number, email address, etc.) of the Objector;

  (ii)   A statement of the Objector's basis for standing; and

  (iii)   A description of the basis for the Objection, including:

    (aa)   A statement of the ground upon which the Objection is being filed, as stated in Article 2(e) of this Procedure;

    (bb)   An explanation of the validity of the Objection and why the objection should be upheld.

(b)   The substantive portion of the Objection shall be limited to 5,000 words or 20 pages, whichever is less, excluding attachments. The Objector shall also describe and provide copies of any supporting or official documents upon which the Objection is based.

(c)   At the same time as the Objection is filed, the Objector shall pay a filing fee in the amount set in accordance with the applicable DRSP Rules and include evidence of such payment in the Objection. In the event that the filing fee is not paid within ten (10) days of the receipt of the Objection by the DRSP, the Objection shall be dismissed without prejudice.

Article 9.   Administrative Review of the Objection

(a)   The DRSP shall conduct an administrative review of the Objection for the purpose of verifying compliance with Articles 5-8 of this Procedure and the applicable DRSP Rules, and inform the Objector, the Applicant and ICANN of the result of its review within fourteen (14) days of its receipt of the Objection. The DRSP may extend this time limit for reasons explained in the notification of such extension.

(b)   If the DRSP finds that the Objection complies with Articles 5-8 of this Procedure and the applicable DRSP Rules, the DRSP shall confirm that the Objection shall be registered for processing.

(c)   If the DRSP finds that the Objection does not comply with Articles 5-8 of this Procedure and the applicable DRSP Rules, the DRSP shall have the discretion to request that any administrative deficiencies in the Objection be corrected within five (5) days. If the deficiencies in the Objection are cured within the specified period but after the lapse of the time limit for submitting an Objection stipulated by Article 7(a) of this Procedure, the Objection shall be deemed to be within this time limit.

(d)   If the DRSP finds that the Objection does not comply with Articles 5-8 of this Procedure and the applicable DRSP Rules, and the deficiencies in the Objection are not corrected within the period specified in Article 9(c), the DRSP shall dismiss the Objection and close the proceedings, without prejudice to the Objector's submission of a new Objection that complies with this Procedure, provided that the Objection is filed within the deadline for filing such Objections. The DRSP's review of the Objection shall not interrupt the running of the time limit for submitting an Objection stipulated by Article 7(a) of this Procedure.

(e)   Immediately upon registering an Objection for processing, pursuant to Article 9(b), the DRSP shall post the following information about the Objection on its website: (i) the proposed string to which the Objection is directed; (ii) the names of the Objector and the Applicant; (ii) the grounds for the Objection; and (iv) the dates of the DRSP's receipt of the Objection.

Article 10.   ICANN's Dispute Announcement

(a)   Within thirty (30) days of the deadline for filing Objections in relation to gTLD applications in a given round, ICANN shall publish a document on its website identifying all of the admissible Objections that have been filed (the "Dispute Announcement"). ICANN shall also directly inform each DRSP of the posting of the Dispute Announcement.

(b)   ICANN shall monitor the progress of all proceedings under this Procedure and shall take steps, where appropriate, to coordinate with any DRSP in relation to individual applications for which objections are pending before more than one DRSP.

Article 11.   Response to the Objection

(a)   Upon receipt of the Dispute Announcement, each DRSP shall promptly send a notice to: (i) each Applicant for a new gTLD to which one or more admissible Objections have been filed with that DRSP; and (ii) the respective Objector(s).

(b)   The Applicant shall file a response to each Objection (the "Response"). The Response shall be filed within thirty (30) days of the Applicant's receipt of the notice sent by the DRSP pursuant to Article 11(a).

(c)   The Response must be filed with the appropriate DRSP, using a model form made available by that DRSP, with copies to ICANN and the Objector.

(d)   The Response shall contain, inter alia, the following information:

(i)   The names and contact information (address, telephone number, email address, etc.) of the Applicant; and

(ii)   A point-by-point response to the statements made in the Objection.

(e)   The substantive portion of the Response shall be limited to 5,000 words or 20 pages, whichever is less, excluding attachments. The Applicant shall also describe and

provide copies of any supporting or official documents upon which the Response is based.

(f)   At the same time as the Response is filed, the Applicant shall pay a filing fee in the amount set and published by the relevant DRSP (which shall be the same as the filing fee paid by the Objector) and include evidence of such payment in the Response. In the event that the filing fee is not paid within ten (10) days of the receipt of the Response by the DRSP, the Applicant shall be deemed to be in default, any Response disregarded and the Objection shall be deemed successful.

(g)   If the DRSP finds that the Response does not comply with Articles 11(c) and (d)(1) of this Procedure and the applicable DRSP Rules, the DRSP shall have the discretion to request that any administrative deficiencies in the Response be corrected within five (5) days. If the administrative deficiencies in the Response are cured within the specified period but after the lapse of the time limit for submitting a Response pursuant to this Procedure, the Response shall be deemed to be within this time limit.

(g)   If the Applicant fails to file a Response to the Objection within the 30-day time limit, the Applicant shall be deemed to be in default and the Objection shall be deemed successful. No fees paid by the Applicant will be refunded in case of default.

Article 12.   Consolidation of Objections

(a)   The DRSP is encouraged, whenever possible and practicable, and as may be further stipulated in the applicable DRSP Rules, to consolidate Objections, for example, when more than one Objector has filed an Objection to the same gTLD on the same grounds. The DRSP shall endeavor to decide upon consolidation prior to issuing its notice pursuant to Article 11(a) and, where appropriate, shall inform the parties of the consolidation in that notice.

(b)   If the DRSP itself has not decided to consolidate two or more Objections, any Applicant or Objector may propose the consolidation of Objections within seven (7) days of the notice given by the DRSP pursuant to Article 11(a). If, following such a proposal, the DRSP decides to consolidate certain Objections, the deadline for the Applicant's Response in the consolidated proceeding shall be thirty (30) days from the Applicant's receipt of the DRSP's notice of consolidation.

(c)   In deciding whether to consolidate Objections, the DRSP shall weigh the benefits (in terms of time, cost, consistency of decisions, etc.) that may result from the consolidation against the possible prejudice or inconvenience that the consolidation may cause.

(d)   Objections based upon different grounds, as summarized in Article 2(e), shall not be consolidated.

Article 13.   The Panel

(a)   The DRSP shall select and appoint the Panel of Expert(s) within thirty (30) days after receiving the Response.

(b)   Number and specific qualifications of Expert(s):

(i)   There shall be one Expert in proceedings involving a String Confusion Objection.

(ii)   There shall be one Expert or, if all of the Parties so agree, three Experts with relevant experience in intellectual property rights disputes in proceedings involving an Existing Legal Rights Objection.

(iii)   There shall be three Experts recognized as eminent jurists of international reputation, one of whom shall be designated as the Chair and of a nationality different from the nationalities of the Applicant and of the Objector, in proceedings involving a Morality and Public Order Objection.

(iv)   There shall be one Expert in proceedings involving a Community Objection.

(c)   All Experts acting under this Procedure shall be impartial and independent of the parties. The applicable DRSP Rules stipulate the manner by which each Expert shall confirm and maintain their impartiality and independence.

(d)   The applicable DRSP Rules stipulate the procedures for challenging an Expert and replacing an Expert.

(e)   Unless required by a court of law or authorized in writing by the parties, an Expert shall not act in any capacity whatsoever, in any pending or future proceedings, whether judicial, arbitral or otherwise, relating to the matter referred to expert determination under this Procedure.

Article 14.   Costs

(a)   Each DRSP shall determine the costs for the proceedings that it administers under this Procedure in accordance with the applicable DRSP Rules. Such costs shall cover the fees and expenses of the members of the Panel, as well as the administrative fees of the DRSP (the "Costs").

(b)   Within ten (10) days of constituting the Panel, the DRSP shall estimate the total Costs and request the Objector and the Applicant/Respondent each to pay in advance the full amount of the Costs to the DRSP. Each party shall make its advance payment of Costs within ten (10) days of receiving the DRSP's request for payment and submit to the DRSP evidence of such payment. The respective filing fees paid by the Parties shall be credited against the amounts due for this advance payment of Costs.

(c)   The DRSP may revise its estimate of the total Costs and request additional advance payments from the parties during the proceedings.

(d)   Failure to make an advance payment of Costs:

(i)   If the Objector fails to make the advance payment of Costs, its Objection shall be dismissed and no fees that it has paid shall be refunded.

(ii)   If the Applicant fails to make the advance payment of Costs, the Objection will be deemed to have been sustained and no fees that the Applicant has paid shall be refunded.

(e)   Upon the termination of the proceedings, after the Panel has rendered its Expert Determination, the DRSP shall refund to the prevailing party, as determined by the Panel, its advance payment(s) of Costs.

Article 15.   Representation and Assistance

(a)   The parties may be represented or assisted by persons of their choice.

(b)   Each party shall communicate the name, contact information and function of such persons to ICANN, the DRSP and the other party (or parties in case of consolidation).

Article 16.   Negotiation and Mediation

(a)   The parties are encouraged, but not required, to participate in negotiations and/or mediation at any time throughout the dispute resolution process aimed at settling their dispute amicably.

(b)   Each DRSP shall be able to propose, if requested by the parties, a person who could assist the parties as mediator.

(c)   A person who acts as mediator for the parties shall not serve as an Expert in a dispute between the parties under this Procedure or any other proceeding under this Procedure involving the same gTLD.

(d)   The conduct of negotiations or mediation shall not, *ipso facto*, be the basis for a suspension of the dispute resolution proceedings or the extension of any deadline under this Procedure. Upon the joint request of the parties, the DRSP or (after it has been constituted) the Panel may grant the extension of a deadline or the suspension of the proceedings. Absent exceptional circumstances, such extension or suspension shall not exceed thirty (30) days and shall not delay the administration of any other Objection.

(e)   If, during negotiations and/or mediation, the parties agree on a settlement of the matter referred to the DRSP under this Procedure, the parties shall inform the DRSP, which shall terminate the proceedings, subject to the parties' payment obligation under this Procedure having been satisfied, and inform ICANN and the parties accordingly.

Article 17.   Additional Written Submissions

(a)   The Panel may decide whether the parties shall submit any written statements in addition to the Objection and the Response, and it shall fix time limits for such submissions.

(b)   The time limits fixed by the Panel for additional written submissions shall not exceed thirty (30) days, unless the Panel, having consulted the DRSP, determines that exceptional circumstances justify a longer time limit.

Article 18.   Evidence

In order to achieve the goal of resolving disputes over new gTLDs rapidly and at reasonable cost, procedures for the production of documents shall be limited. In exceptional cases, the Panel may require a party to provide additional evidence.

Article 19.   Hearings

(a)   Disputes under this Procedure and the applicable DRSP Rules will usually be resolved without a hearing.

(b)   The Panel may decide, on its own initiative or at the request of a party, to hold a hearing only in extraordinary circumstances.

(c)   In the event that the Panel decides to hold a hearing:

   (i)   The Panel shall decide how and where the hearing shall be conducted.

   (ii)   In order to expedite the proceedings and minimize costs, the hearing shall be conducted by videoconference if possible.

   (iii)   The hearing shall be limited to one day, unless the Panel decides, in exceptional circumstances, that more than one day is required for the hearing.

   (iv)   The Panel shall decide whether the hearing will be open to the public or conducted in private.

Article 20.   Standards

(a)   The Panel shall apply the standards that have been defined by ICANN for each category of Objection, and identified in Article 2(e).

(b)   In addition, the Panel may refer to and base its findings upon the statements and documents submitted and any rules or principles that it determines to be applicable.

(c)   The Objector bears the burden of proving that its Objection should be sustained in accordance with the applicable standards.

Article 21.   The Expert Determination

(a)   The DRSP and the Panel shall make reasonable efforts to ensure that the Expert Determination is rendered within forty-five (45) days of the constitution of the Panel. In specific circumstances such as consolidated cases and in consultation with the DRSP, a brief extension may be allowed.

(b)   The Panel shall submit its Expert Determination in draft form to the DRSP's scrutiny as to form before it is signed, unless such scrutiny is specifically excluded by the applicable DRSP Rules. The modifications proposed by the DRSP to the Panel, if any, shall address only the form of the Expert Determination. The signed Expert Determination shall be communicated to the DRSP, which in turn will communicate that Expert Determination to the Parties and ICANN.

(c)   When the Panel comprises three Experts, the Expert Determination shall be made by a majority of the Experts.

(d)   The Expert Determination shall be in writing, shall identify the prevailing party and shall state the reasons upon which it is based. The remedies available to an Applicant or an Objector pursuant to any proceeding before a Panel shall be limited to the success or dismissal of an Objection and to the refund by the DRSP to the prevailing party, as determined by the Panel in its Expert Determination, of its advance payment(s) of Costs pursuant to Article 14(e) of this Procedure and any relevant provisions of the applicable DRSP Rules.

(e)   The Expert Determination shall state the date when it is made, and it shall be signed by the Expert(s). If any Expert fails to sign the Expert Determination, it shall be accompanied by a statement of the reason for the absence of such signature.

(f)   In addition to providing electronic copies of its Expert Determination, the Panel shall provide a signed hard copy of the Expert Determination to the DRSP, unless the DRSP Rules provide for otherwise.

(g)   Unless the Panel decides otherwise, the Expert Determination shall be published in full on the DRSP's website.

Article 22.   Exclusion of Liability

In addition to any exclusion of liability stipulated by the applicable DRSP Rules, neither the Expert(s), nor the DRSP and its employees, nor ICANN and its Board members, employees and consultants shall be liable to any person for any act or omission in connection with any proceeding conducted under this Procedure.

Article 23.   Modification of the Procedure

(a)   ICANN may from time to time, in accordance with its Bylaws, modify this Procedure.

(b)   The version of this Procedure that is applicable to a dispute resolution proceeding is the version that was in effect on the day when the relevant application for a new gTLD is submitted.

[Draft WIPO Rules for New gTLD Dispute Resolution,
Version 1 of August __, 2009]

World Intellectual Property Organization Rules for New gTLD Dispute Resolution for Existing Legal Rights Objections ("WIPO Rules for New gTLD Dispute Resolution")

(In effect as of [Month Date, Year])

1. Scope of WIPO Rules for New gTLD Dispute Resolution in Relation to Procedure

(a) Set out below are the applicable WIPO Rules for New gTLD Dispute Resolution for Existing Legal Rights Objections as referred to in Article [4] of the New gTLD Dispute Resolution Procedure ("Procedure") as approved by the Internet Corporation for Assigned Names and Numbers ("ICANN") on [Month Date, Year]. The WIPO Rules for New gTLD Dispute Resolution are to be read and used in connection with the Procedure which provides the basic framework for the four categories of objections [defined in Article [4] of the Procedure] arising from Applications under ICANN's New gTLD Program.

(b) The version of the WIPO Rules for New gTLD Dispute Resolution applicable to a proceeding conducted under the Procedure is the version in effect on the day when the relevant Application for a new gTLD is submitted. *[Language to be aligned with ultimate language of Article 23(b) of the Procedure.]*

2. Definitions

Terms defined in the Procedure shall have the same meaning in the WIPO Rules for New gTLD Dispute Resolution. Words used in the singular shall include the plural and *vice versa* as the context may require.

3. Communications

(a) Subject to Article [6] of the Procedure, except where otherwise agreed beforehand with the WIPO Arbitration and Mediation Center ("Center"), and subject to the discretion of any appointed Panel, any submission to the Center or to the Panel shall be made:

    (i)   [By electronic mail (email) using [...@wipo.int]; or

    (ii)   In consultation with the Center, and where available, through the WIPO Electronic Case Facility (WIPO ECAF).]

(b) Subject to Article [6(a)] of the Procedure, if a party wishes to submit a hard copy or other non-electronic submission prior to Panel appointment, it shall first request leave to do so from the Center; the Center shall, in its sole discretion, then make a *prima facie* determination whether to accept the non-electronic submission, subject to the ultimate discretion of the Panel on appointment whether to accept the non-electronic submission in accordance with Article [6(a)] of the Procedure.

(c) Absent a request from a party for a hard copy of the Expert Determination, and subject to Article [21(f)] of the Procedure, the Center shall provide the parties and ICANN with an electronic copy of the Expert Determination.

4. Submission of Objection and Response

(a) In accordance with Articles [7] and [8] of the Procedure, the Objector shall transmit its Objection using the Objection Model Form set out in Annex [A] hereto and posted on the Center's website and shall comply with the Center's Filing Guidelines set out in Annex [B] hereto and posted on the Center's website.

(b) In accordance with Article [11] of the Procedure, the Applicant shall transmit its Response using the Response Model Form set out in Annex [C] hereto and posted on the Center's website and shall comply with the Center's Filing Guidelines set out in Annex [B] hereto and posted on the Center's website.

5. Center Review of Objections

(a) In accordance with Article [9] of the Procedure if an Objection is dismissed due to the Objector's failure to remedy an administrative deficiency, there shall be no refund of any DRSP Fee paid by the Objector pursuant to Article [14] of the Procedure and Paragraph [10] of the WIPO Rules for New gTLD Dispute Resolution.

(b) If an Objector submits a new Objection within ten (10) calendar days of closure of a proceeding as provided in Article [9(d)] of the Procedure and Paragraph [5(a)] of the WIPO Rules for New gTLD Dispute Resolution to remedy an administratively deficient Objection, such new Objection may be accompanied by a request for a DRSP Fee waiver, in whole or in part, for the Center's consideration in its sole discretion.

6. Appointment of Case Manager

(a) The Center shall advise the parties of the name and contact details of the Case Manager who shall be responsible for all administrative matters relating to the dispute and communications to the Panel.

(b) The Case Manager may provide administrative assistance to the parties or Panel, but shall have no authority to decide matters of a substantive nature concerning the dispute.

7. Consolidation

(a) In accordance with Article [12] of the Procedure, the Center may, where possible and practicable, and in its sole discretion, decide to consolidate Objections by appointing the same Panel to decide multiple Objections sharing certain commonalities. In the event of consolidation, the Panel shall render individual Expert Determinations for each Objection.

(b) A party may submit a consolidation request pursuant to Article [12(b)] of the Procedure, or may oppose any consolidation request submitted. Any such opposition to a consolidation request shall be provided within seven (7) calendar days of the consolidation request. Any consolidation request or opposition thereto shall be limited to 1,500 words in length.

(c) In the case of consolidated Objections, the applicable reduced Panel fees are specified in Annex [D] hereto and posted on the Center's website.

(d) Pursuant to Article [12] of the Procedure, in weighing the that may result from consolidation against the possible prejudice or inconvenience that consolidation may cause, the Center in reaching its decision concerning consolidation, may take into account, *inter alia*, the following non-exclusive factors:

(i) Whether the Objections concern the same or similar TLD(s);

(ii) Whether the same Objector files Objections concerning multiple TLD applications;

(iii) Whether in any consolidation request, or opposition thereto, the Objector or Applicant relies on single or multiple mark(s);

(iv) The scope of evidence relied on by an Objector or Applicant in any Objection or application;

(v) Any other arguments raised in any consolidation request, or opposition thereto;

(vi) Expert availability to accept appointment.

(e) The Center's decision on any consolidation of multiple Objections for Expert Determination by the same Panel is of an administrative nature and shall be final. The Center shall not be required to state reasons for its decision.

8. Panel Appointment Procedures

(a) The Center will maintain and publish on its website a publicly-available List of Experts.

(b) Pursuant to Article [13(b)(ii)] of the Procedure, there shall be a Single-Expert Panel unless all the Parties agree to the appointment of a Three-Expert Panel.

(c) In the event of a Single-Expert Panel, the Center shall in its sole discretion appoint an Expert from its List of Experts.

(d) In the event all the Parties agree to the appointment of a Three-Expert Panel, any such agreement shall be communicated to the Center within five (5) calendar days of the Center's receipt of the Response filed in accordance with Article [11] of the Procedure and Paragraph [4(b)] of the WIPO Rules for New gTLD Dispute Resolution.

     (i)   If Objections are not consolidated, and if the parties have communicated their agreement on the appointment of a Three-Expert Panel, within five (5) calendar days of such communication each party shall separately submit to the Center (notwithstanding Article [6(b)] of the Procedure) the names of three (3) candidates from the Center's List of Experts, in the order of their respective preference, for appointment by the Center as a Co-Expert. In the event none of a party's three (3) candidates is available for appointment as a Co-Expert, the Center shall appoint the Co-Expert in its sole discretion.

     (ii)   In the event of consolidation in accordance with Paragraph [7] of the WIPO Rules for New gTLD Dispute Resolution, the Objectors or Applicants shall, as the case may be, jointly submit the names of the three (3) candidates from the Center's List of Experts in order of preference (i.e., one list on behalf of all Objector(s) and one list on behalf of all Applicant(s)). If the Objectors or Applicants as the case may be do not jointly agree on and submit the names of three (3) candidates within five (5) calendar days of the parties' communication to the Center on their agreement to the appointment of a Three-Expert Panel, the Center shall in its sole discretion appoint the Co-Experts.

     (iii) The third Expert, who shall be the Presiding Expert, shall absent exceptional circumstances be appointed by the Center from a list of five (5) candidates submitted by the Center to the parties. The Center's selection of a Presiding Expert shall be made in a manner that seeks to reasonably balance the preferences of each party as communicated to the Center within five (5) calendar days of the Center's communication of the list of candidates to the parties.

(iv) Where any party fails to indicate its order of preference for the Presiding Expert to the Center, the Center shall nevertheless proceed to appoint the Presiding Expert in its sole discretion, taking into account any preferences of any other party.

9. Expert Impartiality and Independence

(a) In accordance with Article [13(c)] of the Procedure, any prospective Expert shall, before accepting appointment, disclose to the Center and parties any circumstance that might give rise to justifiable doubt as to the Expert's impartiality or independence, or confirm in writing that no such circumstance exist by submitting to the Center a *Declaration of Impartiality and Independence* using the form set out in Annex [E] hereto and posted on the Center's website.

(b) If at any stage during a proceeding conducted under the Procedure, circumstances arise that might give rise to justifiable doubt as to an Expert's impartiality or independence, the Expert shall promptly disclose such circumstances to the parties and the Center.

(c) A party may challenge an Expert if circumstances exist which give rise to justifiable doubt as to the Expert's impartiality or independence. A party may challenge an Expert whom it has appointed or in whose appointment it concurred, only for reasons of which it becomes aware after the appointment has been made.

(i) A party challenging an Expert shall send notice to the Center and the other party, stating the reasons for the challenge, within five (5) calendar days after being notified of that Expert's appointment or becoming aware of circumstances that it considers give rise to justifiable doubt as to that Expert's impartiality or independence.

(ii) The decision on the challenge shall be made by the Center in its sole discretion. Such a decision is of an administrative nature and shall be final. The Center shall not be required to state reasons for its decision. In the event of an Expert's removal, the Center shall appoint a new Expert in accordance with the Procedure and these WIPO Rules for New gTLD Dispute Resolution.

10. Fees

(a) The applicable fees for the Procedure for Existing Legal Rights Objections are specified in Annex [D] hereto and posted on the Center's website.

(b) After the Expert Determination has been rendered or a proceeding conducted under the Procedure has been terminated, the Center shall provide an accounting to the parties

of the payments received and, in consultation with any Panel, return any unexpended balance of the Panel Fee to the parties.

11. Confidentiality

(a) A party invoking the confidentiality of any information it wishes or is required to submit in any Existing Legal Rights Objection proceeding conducted under the Procedure, shall submit the request for confidentiality to the Center for the Panel's consideration, stating the reasons for which it considers the information to be confidential. If the Panel decides that the information is to be treated as confidential, it shall decide under which conditions and to whom the confidential information may in part or in whole be disclosed and shall require any person to whom the confidential information is to be disclosed to sign an appropriate confidentiality undertaking.

(b) Further to Article [6(b)] of the Procedure, except in exceptional circumstances as decided by the Panel and in consultation with the parties and the Center, no party or anyone acting on its behalf shall have any *ex parte* communication with the Panel.

12. Mediation

Further to Article [16] of the Procedure, prior to the Panel rendering its Expert Determination in a proceeding conducted under the Procedure, the parties may inform the Center that they wish to participate in mediation to attempt to resolve the dispute and may request the Center to administer the mediation. In such event, unless both parties agree otherwise, the WIPO Mediation Rules shall apply *mutatis mutandis*. On request from the parties, and absent exceptional circumstances, the Center's mediation administration fee shall be waived.

13. Effect of Court Proceedings

(a) The Objector and Applicant shall include in any Objection or Response relevant information regarding any other legal proceedings concerning the TLD. In the event that a party initiates any legal proceedings during the pendency of a proceeding conducted under the Procedure, it shall promptly notify the Center.

(b) In the event of any legal proceedings initiated prior to or during a proceeding conducted under the Procedure, the Panel shall have the discretion to decide whether to suspend or terminate such proceeding under the Procedure, or to proceed to an Expert Determination.

14. Termination

(a) If, before the Panel renders an Expert Determination, it becomes unnecessary or impossible to continue a proceeding conducted under the Procedure for any reason, the Panel may in its discretion terminate the proceeding.

(b) If, prior to Panel appointment, it becomes unnecessary or impossible to continue a proceeding conducted under the Procedure for any reason, the Center in consultation with the parties and ICANN, may in its discretion terminate the proceeding.

15. Amendments

Subject to the Procedure, the Center may amend these WIPO Rules for New gTLD Dispute Resolution in its sole discretion.

16. Exclusion of Liability

Except in respect of deliberate wrongdoing, an Expert, the World Intellectual Property Organization, and the Center shall not be liable to any party or ICANN for any act or omission in connection with any proceeding conducted under the Procedure and the WIPO Rules for New gTLD Dispute Resolution.

SCHEDULE OF FEES AND COSTS:
NEW GTLD PRE-DELEGATION LEGAL RIGHTS OBJECTION PROCEDURE
(All amounts are in United States dollars)

(This Schedule may be amended by the DRSP in accordance with its DRSP Rules.)

DRSP Fee[1]

	DRSP Fee
Single-Expert Panel	2,000
Three-Expert Panel	3,000

Panel Fee[2]

Base Panel Fee for Single Objection to Single Application Dispute

Single-Expert Panel	8,000
Three-Expert Panel	20,000
	[Presiding Expert: 10,000, Co-Expert: 5,000]

Panel Fee for Multiple Objections to Single Application:[3]
60% of Regular Base Fee (to be paid per Objection filed)

Single-Expert Panel	4,800
Three-Expert Panel	12,000
	[Presiding Expert: 6,000, Co-Expert: 3,000]

Panel Fee for Multiple Objections filed by Same Objector to Multiple Applications:
80% of Regular Base Fee (to be paid per Objection filed)[3]

Single-Expert Panel	6,400
Three-Expert Panel	16,000
	[Presiding Expert: 8,000, Co-Expert: 4,000]

All Other Scenarios[3]

In all other scenarios, the DRSP shall determine the applicable fees in consultation with the Panel, taking into account the base fees stipulated above and the circumstances of the consolidated objections and applications.

Additional Advance Payments

Depending on the circumstances of the case, additional advance payments may be required to be made. In determining whether additional advance payments shall be required, the DRSP, in consultation with the Panel, may consider the following non-exclusive factors: the number of Applications and/or Objections to the TLD, the number of parties, the complexity of the dispute, the anticipated time required for rendering an Expert Determination, and the possible need for hearings, phone or video conferences, or additional pleading rounds.

---

[1] See Articles 8(c) and 11(f) of the New gTLD Dispute Resolution Procedure.
[2] See Article 14 of the New gTLD Dispute Resolution Procedure.
[3] See Article 12 of the New gTLD Dispute Resolution Procedure.

ICANN

Draft Applicant Guidebook, v3

Module 4

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.

2 October 2009

Module 4

String Contention Procedures

This module describes situations in which contention over applied-for gTLD strings occurs, and the methods available to applicants for resolving such contention cases.

4.1   String Contention

String contention occurs when either:

1. Two or more applicants for an identical gTLD string successfully complete all previous stages of the evaluation and dispute resolution processes; or

2. Two or more applicants for similar gTLD strings successfully complete all previous stages of the evaluation and dispute resolution processes, and the similarity of the strings is identified as creating a probability of user confusion if more than one of the strings is delegated.

ICANN will not approve applications for proposed gTLD strings that are identical or that would result in user confusion, called contending strings. If either situation 1 or 2 above occurs, such applications will proceed to contention resolution through either community priority (comparative) evaluation, in certain cases, or through an auction. Both processes are described in this module. A group of applications for contending strings is referred to as a contention set.

4.1.1   Identification of Contention Sets

Contention sets are groups of applications containing identical or similar applied-for gTLD strings. (In this Applicant Guidebook, "similar" means strings so similar that they create a probability of user confusion if more than one of the strings is delegated into the root zone.) Contention sets are identified during Initial Evaluation following review of all applied-for gTLD strings. ICANN will publish preliminary contention sets by the close of the Initial Evaluation period, and will update the contention sets as necessary during the evaluation and dispute resolution stages.

Applications for identical gTLD strings will be automatically assigned to a contention set. For example, if Applicant A

and Applicant B both apply for .TLDSTRING, they will be identified as being in a contention set. Such testing for identical strings also takes into consideration the code point variants listed in any relevant IDN table.

The String Similarity Panel will also review the entire pool of applied-for strings to determine whether the strings proposed in any two or more applications are so similar that they would create a probability of user confusion if allowed to coexist in the DNS. The panel will make such a determination for each pair of applied-for gTLD strings. The outcome of the String Similarity Review described in subsection 2.1.1.1 of Module 2 is the identification of contention sets among applications that have direct or indirect contention relationships with one another.

Additionally, an applicant may file a String Confusion objection (described in Module 3) against another application alleging that the applied-for string is so similar to its own that the delegation of both would create a probability of user confusion. If the objection is upheld, the contention set will be augmented (see subsection 4.1.2 below).

Two strings are in **direct contention** if they are identical or so similar that there is a probability of user confusion if both were to be delegated as TLDs in the root zone. More than two applicants might be represented in a direct contention situation: if four different applicants applied for the same gTLD string, they would all be in direct contention with one another.

Two strings are in **indirect contention** if they are both in direct contention with a third string, but not with one another. The example that follows explains direct and indirect contention in greater detail.

In Figure 4-1, Strings A and B are an example of direct contention. Strings C and G are an example of indirect contention. C and G both contend with B, but not with one another. The figure as a whole is one contention set. A contention set consists of all applications that are linked by string contention to one another, directly or indirectly.
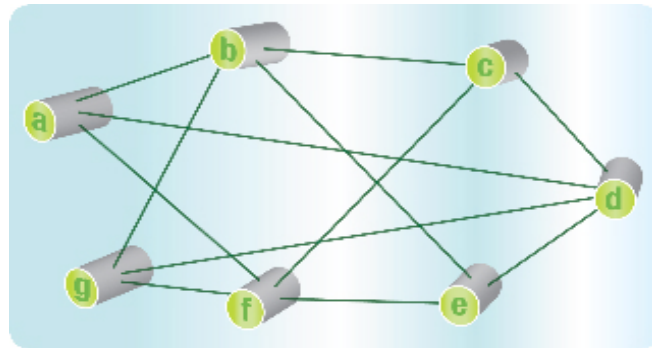
Figure 4-1 – This diagram represents one contention set, featuring both directly and indirectly contending strings.

While preliminary contention sets are determined during Initial Evaluation, the final configuration of the contention sets can only be established once the evaluation and dispute resolution process stages have concluded. This is because any application excluded through those processes might modify a contention set identified earlier. A contention set may be split into two sets or it may be eliminated altogether as a result of an Extended Evaluation or dispute resolution proceeding.

Refer to Figure 4-2: In contention set 1, applications D and G are eliminated. Application A is the only remaining application, so there is no contention left to resolve.

In contention set 2, all applications successfully complete Extended Evaluation and Dispute Resolution, so the original contention set remains to be resolved.

In contention set 3, application F is eliminated. Since application F was in direct contention with E and J, but E and J are not in contention with one other, the original contention set splits into two sets: one containing E and K in direct contention, and one containing I and J.
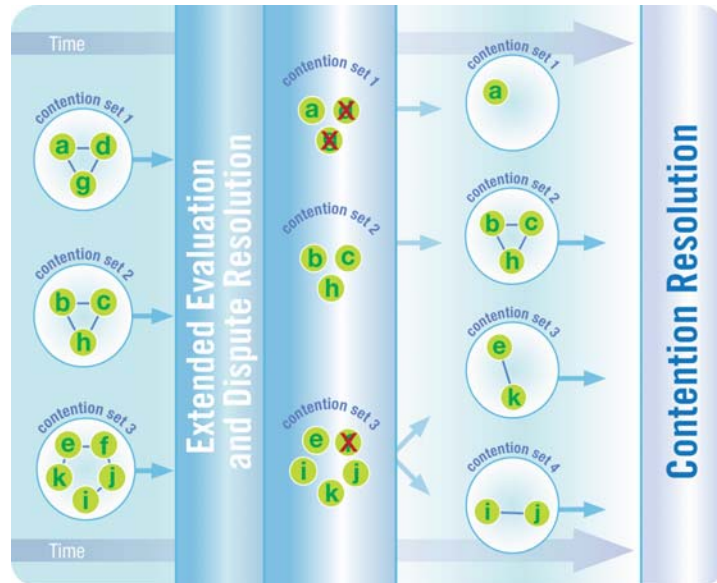
Figure 4-2 – Resolution of string contention cannot begin until all applicants within a contention set have completed all applicable previous stages.

The remaining contention cases must then be resolved through community priority (comparative) evaluation or by other means, depending on the circumstances. In the string contention resolution stage, ICANN addresses each contention set to achieve an unambiguous resolution.

As described elsewhere in this document, cases of contention might be resolved by community priority (comparative) evaluation or some agreement among the parties. Absent that, the last-resort contention resolution mechanism will be an auction.

4.1.2 *Impact of Dispute Resolution Proceedings on Contention Sets*

If an applicant files a string confusion objection against another application (refer to Module 3), and the panel finds that user confusion is probable (that is, finds in favor of the objector), the two applications will be placed in direct contention with each other. Thus, the outcome of a dispute resolution proceeding based on a string confusion objection would be a new contention set structure for the relevant applications.

If an applicant files a string confusion objection against another application, and the panel finds that string

confusion does not exist (that is, finds in favor of the responding applicant), the two applications may both move forward and will not be considered in direct contention with one another.

A dispute resolution outcome will not result in removal of an application from an earlier identified contention set.

4.1.3   Self-Resolution of String Contention

Applicants that are identified as being in contention are encouraged to reach a settlement or agreement among themselves that resolves the contention. This may occur at any stage of the process, once ICANN publicly posts the applications received on its website.

Applicants may resolve string contention in a manner whereby one or more applicants withdraw their applications. An applicant may not resolve string contention by selecting a new string or by replacing itself with a joint venture. It is understood that joint ventures may result from self-resolution of string contention by applicants. However, material changes in applications (for example, combinations of applicants to resolve contention) will require re-evaluation. This might require additional fees or evaluation in a subsequent application round. Applicants are encouraged to resolve contention by combining in a way that does not materially affect the remaining application.

4.1.4   Possible Contention Resolution Outcomes

An application that has successfully completed all previous stages and is no longer part of a contention set due to changes in the composition of the contention set (as described in subsection 4.1.1) or self-resolution by applicants in the contention set (as described in subsection 4.1.3) may proceed to the next stage.

An application that prevails in a contention resolution procedure, either community priority (comparative) evaluation or auction, may proceed to the next stage.

In some cases, an applicant who is not the outright winner of a string contention resolution process can still proceed. This situation is explained in the following paragraphs.

If the strings within a given contention set are all identical, the applications are in direct contention with each other

and there can only be one winner that proceeds to the next step.

However, where there are both direct and indirect contention situations within a set, more than one string may survive the resolution.

For example, consider a case where string A is in contention with B, and B is in contention with C, but C is not in contention with A. If A wins the contention resolution procedure, B is eliminated but C can go on since C is not in direct contention with the winner and both strings can coexist in the DNS without risk for confusion.

4.2   Community Priority (Comparative) Evaluation

Community priority (comparative) evaluation will only occur if a community-based applicant selects this option. Community priority (comparative) evaluation can begin once all applications in the contention set have completed all previous stages of the process.

The community priority (comparative) evaluation is an independent analysis. Scores received in the applicant reviews are not carried forward to the community priority (comparative) evaluation. Each application participating in the community priority (comparative) evaluation begins with a score of zero.

4.2.1   Eligibility for Community Priority (Comparative) Evaluation

As described in subsection 1.2.2 of Module 1, all applicants are required to identify whether their application type is:

- Community-based; or

- Standard.

Applicants designating their applications as community-based are also asked to respond to a set of questions in the application form to provide relevant information if a community priority (comparative) evaluation occurs.

Only community-based applicants are eligible to participate in a community priority (comparative) evaluation.

At the start of the contention resolution stage, all community-based applicants within remaining contention sets will be notified of the opportunity to opt for a community priority (comparative) evaluation via submission of a deposit by a specified date. Only those applications for which a deposit has been received by the deadline will be scored in the community priority (comparative) evaluation.

Before the community priority (comparative) evaluation begins, the applicants who have elected to participate may be asked to provide additional information relevant to the community priority (comparative) evaluation. Following the evaluation, the deposit will be refunded to applicants that score 14 or higher.

4.2.2 *Community Priority (Comparative) Evaluation Procedure*

Community priority (comparative) evaluations for each eligible contention set will be performed by a community priority panel appointed by ICANN to review contending applications. The panel's role is to determine whether any of the community-based applications fulfills the community priority criteria. Standard applicants within the contention set, if any, will not participate in the community priority (comparative evaluation).

If a single community-based application is found to meet the community priority criteria (see subsection 4.2.3 below), that applicant will be declared to prevail in the community priority (comparative) evaluation and may proceed. If more than one community-based application is found to meet the criteria, the remaining contention between them will be resolved as follows:

- In the case where the applications are in <u>indirect contention</u> with one another (see subsection 4.1.1), they will both be allowed to proceed to the next stage. In this case, applications that are in direct contention with any of these community-based applications will be eliminated.

- In the case where the applications are in <u>direct contention</u> with one another, these applicants will proceed to an auction. If all parties agree and present a joint request, ICANN may postpone the auction for a three-month period while the parties attempt to reach a settlement before proceeding

to auction. This is a one-time option; ICANN will grant no more than one such request for each set of contending applications.

If none of the community-based applications are found to meet the criteria, then all of the parties in the contention set (both standard and community-based applicants) will proceed to an auction.

4.2.3 *Community Priority (Comparative) Evaluation Criteria*

The Community Priority Panel will review and score the one or more community-based applications having elected the community priority (comparative) evaluation against four criteria as listed below.

The scoring process is conceived to identify qualified community-based applications, while preventing both "false positives" (awarding undue priority to an application that refers to a "community" construed merely to get a sought-after generic word as a gTLD string) and "false negatives" (not awarding priority to a qualified community application). This calls for a holistic approach, taking multiple criteria into account, as reflected in the process.

It should be noted that a qualified community application eliminates all directly contending standard applications, regardless of how well qualified the latter may be. This is a fundamental reason for very stringent requirements for qualification of a community-based application, as embodied in the criteria below.

An application must score at least 14 points to prevail in a community priority (comparative) evaluation. The outcome will be determined according to the procedure described in subsection 4.2.2.

Criterion #1: Community Establishment (0-4 points)

A maximum of 4 points is possible on the Community Establishment criterion:

4	3	2	1	0
Community Establishment				

High ⬅————————➡ Low
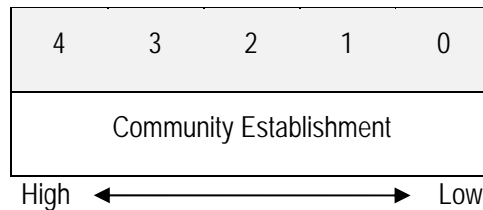
As measured by:

A. Delineation (2)

2	1	0
Clearly delineated, organized, and pre-existing community.	Clearly delineated and pre-existing community, but not fulfilling the requirements for a score of 2.	Insufficient delineation and pre-existence for a score of 1.

B. Extension (2)

2	1	0
Community of considerable size and longevity.	Community of either considerable size or longevity, but not fulfilling the requirements for a score of 2.	Community of neither considerable size nor longevity.

Explanatory notes: Usage of the expression "community" has evolved considerably from its Latin origin – "communitas" meaning "fellowship" – while still implying more of cohesion than a mere commonality of interest. Notably, there should be an awareness and recognition of a community among its members.

The scoring for this criterion relates to the community as explicitly addressed according to the application. It should be noted that a community can consist of legal entities (for example, an association of suppliers of a particular service), of individuals (for example, a language community) or of a logical alliance of communities (for example, an international federation of national communities of a similar nature). All are viable as such, provided the requisite awareness and recognition of the community is at hand among the members. Otherwise the application would be seen as not relating to a real community and score 0 on both delineation and extension above. If in doubt in this or other respects regarding an

application, the panel may use information sources outside the application itself to verify the circumstances.

"Delineation" relates to the membership of a community, where a clear and straight-forward membership definition scores high, while an unclear, dispersed or unbound definition scores low. "Pre-existing" means that a community has been active as such since before the new gTLD policy recommendations were completed in September 2007. "Organized" implies that there is at least one entity dedicated to the community, with documented evidence of community activities.

"Size" relates both to the number of members and the geographical reach of the community and will be scored depending on the context rather than on absolute numbers - a geographic location community may count millions of members in a limited location, a language community may have a million members with some spread over the globe, a community of service providers may have "only" some hundred members although well spread over the globe, just to mention some examples - all these can be regarded as of "considerable size". "Longevity" means that the pursuits of a community are of a lasting, non-transient nature.

Criterion #2: Nexus between Proposed String and Community (0-4 points)

A maximum of 4 points is possible on the Nexus criterion:

4	3	2	1	0
Nexus between String & Community				

High ⟵⟶ Low
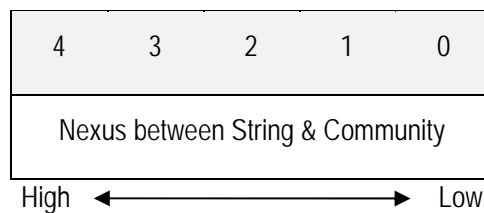
As measured by:

A. Nexus (3)

3	2	0
The string matches the name of the community or is a well known short-form or	String identifies the community, but does not qualify for a score of 3.	String nexus does not fulfill the requirements for a score of 2.

3	2	0
abbreviation of the community name.		

B. Uniqueness (1)

1	0
String has no other significant meaning beyond identifying the community.	String does not fulfill the requirement for a score of 1.

Explanatory notes:

For a score of 3 on A: "Name" of the community means the established name by which the community is commonly known by others. It may be, but does not need to be, the name of an organization dedicated to the community. The essential aspect is that the name is commonly known by others as the identification of the community.

For a score of 2 on A: A string "identifies" the community if it closely describes the community or the community members, without over-reaching beyond the community. As an example, a string could qualify for a score of 2 if it is a noun that the typical community member would naturally be called in the context.

Regarding B: "Significant meaning" relates to the public in general, with consideration of the community language context added. "Uniqueness" will be scored both with regard to the community context and from a general point of view. For example, a string for a particular geographic location community may seem unique from a general perspective, but would not score a 1 for uniqueness if it carries another significant meaning in the common language used in the relevant community location. The phrasing "...beyond identifying the community" in the score of 1 for "uniqueness" implies a requirement that the string does identify the community, i.e. scores 2 or 3 for "Nexus", in order to be eligible for a score of 1 for "Uniqueness".

Criterion #3: Registration Policies (0-4 points)

A maximum of 4 points is possible on the Registration
Policies criterion:

4	3	2	1	0
Registration Policies				

High ←—————————————→ Low

As measured by:

A. Eligibility (1)

1	0
Eligibility restricted to community members.	Largely unrestricted approach to eligibility.

B. Name selection (1)

1	0
Policies include name selection rules consistent with the articulated community-based purpose of the applied-for gTLD.	Policies do not fulfill the requirements for a score of 1.

C. Content and use (1)

1	0
Policies include rules for content and use consistent with the articulated community-based purpose of the applied-for gTLD.	Policies do not fulfill the requirements for a score of 1.

D. Enforcement (1)

1	0
Policies include specific enforcement measures (e.g. investigation practices, penalties, takedown procedures) constituting a coherent set with appropriate appeal mechanisms.	Policies do not fulfill the requirements for a score of 1.

Explanatory notes:

Regarding A: The limitation to community "members" can invoke a formal membership but can also be satisfied in other ways, depending on the structure and orientation of the community at hand. For example, for a geographic location community TLD a limitation to members of the community can be achieved by requiring that the registrant's physical address is within the boundaries of the location.

Regarding B, C and D: Scoring of applications against these sub-criteria will be done from a holistic perspective, with due regard for the particularities of the community explicitly addressed. For example, an application proposing a TLD for a language community may feature strict rules imposing this language for name selection as well as for content and use, scoring 1 on both B and C above. It could nevertheless include forbearance in the enforcement measures for tutorial sites assisting those wishing to learn the language and still score 1 on D.

Criterion #4: Community Endorsement (0-4 points)

A maximum of 4 points is possible on the Community Endorsement criterion:

4	3	2	1	0
Community Endorsement				

High ⟷ Low
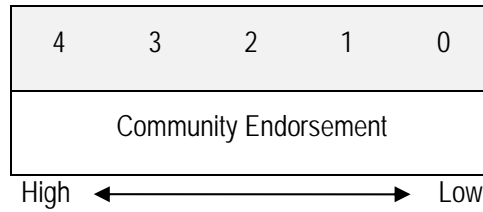
As measured by:

A. Support (2)

2	1	0
Applicant is, or has documented support from, the recognized community institution(s)/ member organization(s) or has otherwise documented authority to represent the community.	Documented support from at least one group with relevance, but insufficient support for a score of 2.	Insufficient proof of support for a score of 1.

B.   Opposition (2)

2	1	0
No opposition of relevance.	Relevant opposition from at least one group of non-negligible size.	Strong and relevant opposition.

Explanatory notes: Support and opposition will be scored in relation to the communities explicitly addressed as stated in the application with due regard taken to the communities implicitly addressed by the string. It follows that support from, for example, the only national association relevant to a particular community on a national level would score a 2 if the string is clearly orientated to that national level, but only a 1 if the string implicitly addresses similar communities in other nations. However, it should be noted that documented support from groups or communities that may be seen as implicitly

addressed but have completely different orientations compared to the applicant community will not be required for a score of 2 regarding support.

"Recognized" means the institution(s)/organization(s) that, through membership or otherwise, are clearly recognized by the community members as representative of the community. The plurals in brackets relate to cases of alliances of multiple communities. In such cases, a score of "2" calls for documented support from institutions/organizations representing a majority of the overall community addressed.

"Relevance" and "relevant" refer to the communities explicitly and implicitly addressed. This means that opposition from communities implicitly addressed by the string would be considered relevant.

Previous objections to the application during the same application round will be taken into account when scoring "Opposition" and be assessed in this context without any presumption that such objections would lead to a particular score.

4.3 Auction: Mechanism of Last Resort

It is expected that most cases of contention will be resolved by the community priority (comparative) evaluation, or through voluntary agreement among the involved applicants. Auction is a tie-breaker method for resolving string contention among the applications within a contention set, if the contention has not been resolved by other means.

In practice, ICANN expects that most contention cases will be resolved through other means before reaching the auction stage. There is a possibility that significant funding will accrue to ICANN as a result of one or more auctions. [1]

---

[1] The purpose of an auction is to resolve contention in a clear, objective manner. Proceeds from auctions will be reserved and earmarked until the uses of the proceeds are determined. It is planned that costs of the new gTLD program will offset by fees, so any funds coming from a last resort contention resolution mechanism such as auctions would result (after paying for the auction process) in additional funding. Therefore, consideration of a last resort contention mechanism should include the uses of funds. Funds must be earmarked separately and used in a manner that supports directly ICANN's Mission and Core Values and also maintains its not for profit status.

Possible uses include formation of a foundation with a clear mission and a transparent way to allocate funds to projects that are of interest to the greater Internet community, such as grants to support new gTLD applications or registry operators from communities

4.3.1 Auction Procedures

An auction of two or more applications within a contention set is conducted as follows. The auctioneer successively increases the prices associated with applications within the contention set, and the respective applicants indicate their willingness to pay these prices. As the prices rise, applicants will successively choose to exit from the auction. When a sufficient number of applications have been eliminated so that no direct contentions remain (i.e., the remaining applications are no longer in contention with one another and can all be delegated), the auction will be deemed to conclude. At the auction's conclusion, the remaining applications will pay the resulting prices and proceed toward delegation. This procedure is referred to as an "ascending-clock auction."

This section provides applicants an informal introduction to the practicalities of participation in an ascending-clock auction. It is intended only as a general introduction and is only preliminary. If conflict arises between this section and the auction rules issued prior to commencement of any auction proceedings, the auction rules will prevail. For simplicity, this section will describe the situation where a contention set consists of two or more applications for identical strings.

All auctions will be conducted over the Internet, with participants placing their bids remotely using a web-based software system designed especially for auction. The auction software system will be compatible with current versions of most prevalent browsers, and will not require the local installation of any additional software.

Auction participants ("bidders") will receive instructions for access to the online auction site. Access to the site will be password-protected and bids will be encrypted through SSL. If a bidder temporarily loses connection to the Internet, that bidder may be permitted to submit its bids in a given auction round by fax, according to procedures described

in subsequent gTLD rounds, the creation of an ICANN-administered/community-based fund for specific projects for the benefit of the Internet community, the creation of a registry continuity fund for the protection of registrants (ensuring that funds would be in place to support the operation of a gTLD registry until a successor could be found), or establishment of a security fund to expand use of secure protocols, conduct research, and support standards development organizations in accordance with ICANN's security and stability mission.

Further detail on the potential uses of funds will be provided with the proposed budget for the new gTLD process and updated Applicant Guidebook materials.

in the auction rules. The auctions will generally be conducted to conclude quickly, ideally in a single day.

The auction will be carried out in a series of auction rounds, as illustrated in Figure 4-3. The sequence of events is as follows:

1. For each auction round, the auctioneer will announce in advance: (1) the start-of-round price, (2) the end-of-round price, and (3) the starting and ending times of the auction round. In the first auction round, the start-of-round price for all bidders in the auction will be USD 0. In later auction rounds, the start-of-round price will be its end-of-round price from the previous auction round.
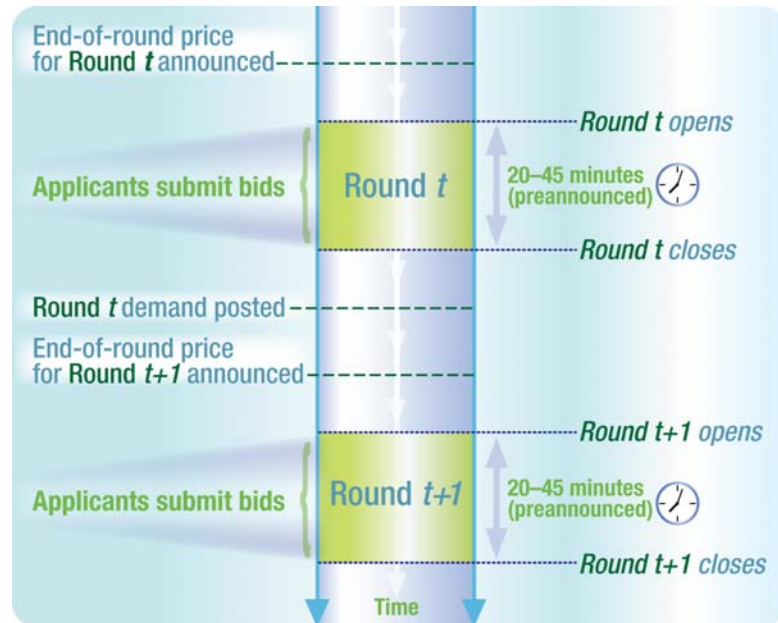
Figure 4-3 – Sequence of events during an ascending-clock auction.

2. During each auction round, bidders will be required to submit a bid or bids representing their willingness to pay within the range of intermediate prices between the start-of-round and end-of-round prices. In this way a bidder indicates its willingness to stay in the auction at all prices through and including the end-of-auction round price, or its wish to exit the auction at a price less than the end-of-auction round price, called the exit bid.

3. Exit is irrevocable. If a bidder exited the auction in a previous auction round, the bidder is not permitted to re-enter in the current auction round.

4. Bidders may submit their bid or bids at any time during the auction round.

5. Only bids that comply with all aspects of the auction rules will be considered valid. If more than one valid bid is submitted by a given bidder within the time limit of the auction round, the auctioneer will treat the last valid submitted bid as the actual bid.

6. At the end of each auction round, bids become the bidders' legally-binding offers to secure the relevant gTLD strings at prices up to the respective bid amounts, subject to closure of the auction in accordance with the auction rules. In later auction rounds, bids may be used to exit from the auction at subsequent higher prices.

7. After each auction round, the auctioneer will disclose the aggregate number of bidders remaining in the auction at the end-of-round prices for the auction round, and will announce the prices and times for the next auction round.

   • Each bid should consist of a single price associated with the application, and such price must be greater than or equal to the start-of-round price.

   • If the bid amount is strictly less than the end-of-round price, then the bid is treated as an exit bid at the specified amount, and it signifies the bidder's binding commitment to pay up to the bid amount if its application is approved.

   • If the bid amount is greater than or equal to the end-of-round price, then the bid signifies that the bidder wishes to remain in the auction at all prices in the current auction round, and it signifies the bidder's binding commitment to pay up to the end-of-round price if its application is approved. Following such bid, the application cannot be eliminated within the current auction round.

   • To the extent that the bid amount exceeds the end-of-round price, then the bid is also treated as a proxy bid to be carried forward to the next auction

round. The bidder will be permitted to change the proxy bid amount in the next auction round, and the amount of the proxy bid will not constrain the bidder's ability to submit any valid bid amount in the next auction round.

- No bidder is permitted to submit a bid for any application for which an exit bid was received in a prior auction round. That is, once an application has exited the auction, it may not return.

- If no valid bid is submitted within a given auction round for an application that remains in the auction, then the bid amount is taken to be the amount of the proxy bid, if any, carried forward from the previous auction round or, if none, the bid is taken to be an exit bid at the start-of-round price for the current auction round.

8. This process continues, with the auctioneer increasing the price range for each given TLD string in each auction round, until there is one remaining bidder at the end-of-round price. After an auction round in which this condition is satisfied, the auction concludes and the auctioneer determines the clearing price. The last remaining application is deemed the successful application, and the associated bidder is obligated to pay the clearing price.

Figure 4-4 illustrates how an auction for five contending applications might progress.
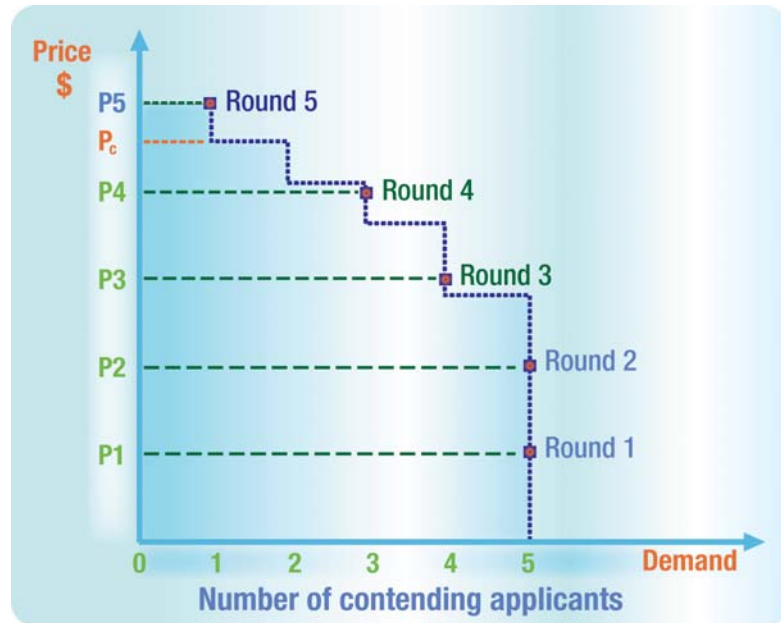
Figure 4-4 – Example of an auction for five mutually-contending applications.

- Before the first auction round, the auctioneer announces the end-of-round price P_1.

- During Auction round 1, a bid is submitted for each application. In Figure 4-4, all five bidders submit bids of at least P_1. Since the aggregate demand exceeds one, the auction proceeds to Auction round 2. The auctioneer discloses that five contending applications remained at P_1 and announces the end-of-round price P_2.

- During Auction round 2, a bid is submitted for each application. In Figure 4-4, all five bidders submit bids of at least P_2. The auctioneer discloses that five contending applications remained at P_2 and announces the end-of-round price P_3.

- During Auction round 3, one of the bidders submits an exit bid at slightly below P_3, while the other four bidders submit bids of at least P_3. The auctioneer discloses that four contending applications remained at P_3 and announces the end-of-round price P_4.

- During Auction round 4, one of the bidders submits an exit bid midway between P_3 and P_4, while the other three remaining bidders submit bids of at least P_4. The auctioneer discloses that three contending applications remained at P_4 and announces the end-of-auction round price P_5.

- During Auction round 5, one of the bidders submits an exit bid at slightly above P_4, and one of the bidders submits an exit bid at P_c midway between P_4 and P_5. The final bidder submits a bid greater than P_c. Since the aggregate demand at P_5 does not exceed one, the auction concludes in Auction round 5. The application associated with the highest bid in Auction round 5 is deemed the successful application. The clearing price is P_c, as this is the lowest price at which aggregate demand can be met.

To the extent possible, auctions to resolve multiple string contention situations may be conducted simultaneously.

4.3.1.1   Currency

For bids to be comparable, all bids in the auction will be submitted in any integer (whole) number of US dollars.

4.3.1.2   Fees

A bidding deposit will be required of applicants participating in the auction, in an amount to be determined. The bidding deposit must be transmitted by wire transfer to a specified bank account specified by ICANN or its auction provider at a major international bank, to be received in advance of the auction date. The amount of the deposit will determine a bidding limit for each bidder: the bidding deposit will equal 10% of the bidding limit; and the bidder will not be permitted to submit any bid in excess of its bidding limit.

In order to avoid the need for bidders to pre-commit to a particular bidding limit, bidders may be given the option of making a specified deposit that will provide them with unlimited bidding authority for a given application. The amount of the deposit required for unlimited bidding authority will depend on the particular contention set and will be based on an assessment of the possible final prices within the auction.

All deposits from nondefaulting losing bidders will be returned following the close of the auction.

4.3.2   Winning Bid Payments

Any applicant that participates in an auction will be required to sign a bidder agreement that acknowledges its rights and responsibilities in the auction, including that its bids are legally binding commitments to pay the amount bid if it wins (i.e., if its application is approved), and to enter into the prescribed registry agreement with ICANN— together with a specified penalty for defaulting on payment of its winning bid or failing to enter into the required registry agreement.

The winning bidder in any auction will be required to pay the full amount of the final price within 20 business days of the end of the auction. Payment is to be made by wire transfer to the same international bank account as the bidding deposit, and the applicant's bidding deposit will be credited toward the final price.

In the event that a bidder anticipates that it would require a longer payment period than 20 business days due to verifiable government-imposed currency restrictions, the bidder may advise ICANN well in advance of the auction and ICANN will consider applying a longer payment period to all bidders within the same contention set.

Any winning bidder for whom the full amount of the final price is not received within 20 business days of the end of an auction is subject to being declared in default. At their sole discretion, ICANN and its auction provider may delay the declaration of default for a brief period, but only if they are convinced that receipt of full payment is imminent.

Any winning bidder for whom the full amount of the final price is received within 20 business days of the end of an auction retains the obligation to execute the required registry agreement within 90 days of the end of auction. Such winning bidder who does not execute the agreement within 90 days of the end of the auction is subject to being declared in default. At their sole discretion, ICANN and its auction provider may delay the declaration of default for a brief period, but only if they are convinced that execution of the registry agreement is imminent.

4.3.3   Post-Default Procedures

Once declared in default, any winning bidder is subject to immediate forfeiture of its position in the auction and assessment of default penalties. After a winning bidder is declared in default, the remaining bidders will receive an offer to have their applications accepted, one at a time, in descending order of their exit bids. In this way, the next bidder would be declared the winner subject to payment of its last bid price.

Each bidder that is offered the relevant gTLD will be given a specified period—typically, four business days—to respond as to whether it wants the gTLD. A bidder who responds in the affirmative will have 20 business days to submit its full payment. The penalty for defaulting on a winning bid will equal 10% of the defaulting bid.[2]

Default penalties will be charged against any defaulting applicant's bidding deposit before the associated bidding deposit is returned.

4.4 Contention Resolution and Contract Execution

An applicant that has been declared the winner of a contention resolution process will proceed by entering into the contract execution step. (Refer to section 5.1 of Module 5.)

If a winner of the contention resolution procedure has not executed a contract within 90 days of the decision, ICANN has the right to extend an offer to the runner-up applicant, if any, to proceed with its application. For example, in an auction, another applicant who would be considered the runner-up applicant might proceed toward delegation. This offer is at ICANN's option only. The runner-up applicant in a contention resolution process has no automatic right to an applied-for gTLD string if the first place winner does not execute a contract within a specified time.

---

[2] If bidders were given the option of making a specified deposit that provided them with unlimited bidding authority for a given application and if the winning bidder utilized this option, then the penalty for defaulting on a winning bid will be the lesser of the following: (1) 10% of the defaulting bid, or (2) the specified deposit amount that provided the bidder with unlimited bidding authority.

DRAFT - New gTLD Program - String Contention

Application/Admin Check

- Applicant begins application process
- If applicant is community based, must elect whether they choose community priority evaluation in the event of string contention
- Applicant completes application process in TLD Application System (TAS)
- ICANN publishes list of all applications
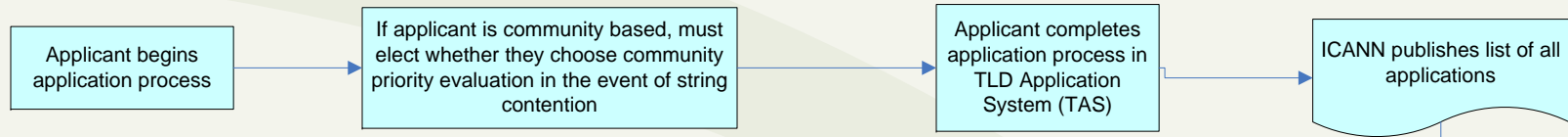
Initial Evaluation (IE) String Review

- Algorithm run by ICANN for all applied-for gTLDs against all other applied-for gTLDs
- String Similarity Panel uses algorithm results and analysis to group similar and identical strings into Contention Sets

IE + EE + Dispute Res

- IE, Extended Evaluation (EE), and Dispute Resolution continue. Some applications may not pass certain elements of the review process, *which may alter the contention sets.*

String Contention

- Is the applied-for gTLD in a contention set?
  - NO
  - Yes
- Applicants are encouraged to self-resolve string contention anytime prior to or during the evaluation process
- Have one or more community-based applicant(s) elected community priority evaluation?
  - YES
  - NO
- Community priority evaluation
- Does one clear winner emerge?
  - NO
  - YES
- Applicants with contending strings participate in auction: One or more parties proceed to subsequent stage

Transition to Delegation

- Applicant enters Transition to Delegation phase

DRAFT – For Discussion Purposes - Aug 09 v1.61

ICANN

Draft Applicant Guidebook, v3

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.

2 October 2009

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 in order to proceed 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.

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 registry 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 as described in the Evaluation Criteria.

5-1

Draft Applicant Guidebook v3 – For Discussion Only

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 on-site at the services delivery point of the registry.

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 DNSSEC Policy Statement (DPS);

5-2

- Its executed agreement with its selected escrow agent; and

- 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 communicate with the applicant.

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

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.

System performance requirements -- 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 network and server capacity available and an estimate of expected capacity 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 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 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 for each applicant-listed name server. 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 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, 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

5-4

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. ICANN will review the self-certification materials as well as test the reachability and DNS transaction capacity for DNS queries using the EDNS(0) protocol extension for each name server. In case of use of anycast, each individual server in each anycast set will be tested.

Load capacity, latency and reachability shall be documented as for 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 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 Whois data is accessible via both port 43 and via a web interface and review self-certification documentation regarding Whois transaction capacity. Access to Whois (both port 43 and via the web) will be tested by ICANN remotely from various points on the Internet.

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 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. 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, both one full and one incremental, 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 recovered and the registry reconstituted to the point where it can respond to DNS and Whois queries (both via port 43 and via the web) should it be necessary.

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. Information about the delegation process is available at http://iana.org/domains/root/.

5-7

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[1] (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

---

[1] 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)[2] following the process in Annex A of the ICANN Bylaws.[3] The policy development process involves deliberation and collaboration by the various 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.

---

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

Implement rights protection measures. The registry operator is 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).

Implement measures for protection of 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 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.)

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 will also perform audits 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.

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.

New gTLD Agreement

Proposed Draft (v.3)

This document contains the draft registry agreement associated with the Draft Applicant Guidebook (Draft RFP) for New gTLDs.

Successful gTLD applicants would enter into this form of registry agreement with ICANN prior to delegation of the new gTLD. Background information on how this version of the draft agreement differs from the previous draft (see http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-18feb09-en.pdf) is available in the explanatory memorandum *Summary of Changes to Base Agreement.*

It is important to note that this draft agreement does not constitute a formal position by ICANN, and has not been approved by ICANN's Board of Directors. The agreement is being set out for review and community discussion purposes, and ICANN encourages comments and suggestions for improvement. 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.

REGISTRY AGREEMENT

This REGISTRY AGREEMENT (this "Agreement") is entered into as of _____ (the "Effective Date") between Internet Corporation for Assigned Names and Numbers, a California nonprofit public benefit corporation ("ICANN"), and _____ a _____ ("Registry Operator").

ARTICLE 1.

DELEGATION AND OPERATION
OF TOP–LEVEL DOMAIN; REPRESENTATIONS AND WARRANTIES

1.1 **Domain and Designation.** The Top-Level Domain to which this Agreement applies is ____ (the "TLD"). Upon the Effective Date and until the end of the Term (as defined in Section 4.1), ICANN designates _____ as the registry operator for the TLD, subject to the requirements and necessary approvals for delegation of the TLD and entry into the root-zone.

1.2 **Technical Feasibility of String.** While ICANN has encouraged and will continue to encourage universal acceptance of all top-level domain strings across the Internet, certain top-level domain strings may encounter difficulty in acceptance by ISPs and webhosters and/or validation by web applications. Registry Operator shall be responsible for ensuring to its satisfaction the technical feasibility of the TLD string prior to entering into this Agreement.

1.3 **Representations and Warranties.**

(a) Registry Operator represents and warrants to ICANN as follows:

(i) all material information provided and statements made in the registry TLD application, and statements made in writing during the negotiation of this Agreement, were true and correct in all material respects at the time made, and such information or statements continue to be true and correct in all material respects as of the Effective Date except as otherwise previously disclosed in writing by Registry Operator to ICANN;

(ii) Registry Operator is a _____, duly organized, validly existing and in good standing under the laws of _____, and Registry Operator has all requisite power and authority and obtained all necessary _____ approvals to enter into and duly execute and deliver this Agreement; and

(iii) Each of Registry Operator and the other parties thereto has duly executed and delivered to ICANN an instrument that secures the funds required to perform registry functions for the TLD in the event of the termination or expiration of this Agreement (the "Continued Operations Instrument"), and such instrument is a binding obligation of the parties thereto, enforceable against the parties in accordance with its terms.

(b) ICANN represents and warrants to Registry Operator that ICANN is a nonprofit public benefit corporation duly organized, validly existing and in good standing under the laws of the State of California, United States of America. ICANN has all requisite power and authority and obtained all necessary corporate approvals to enter into and duly execute and deliver this Agreement.

---

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

ARTICLE 2.

COVENANTS OF REGISTRY OPERATOR

Registry Operator covenants and agrees with ICANN as follows:

2.1   Approved Services; Additional Services. Registry Operator shall be entitled to provide the Registry Services described in clauses (a) and (b) of the first paragraph of Section 2 in Specification 6 at [*see specification 6*]) and such other Registry Services set forth on Exhibit A (collectively, the "Approved Services"). If Registry Operator desires to provide any Registry Service that is not an Approved Service or is a modification to an Approved Service (each, an "Additional Service"), Registry Operator shall submit requests for approval of such Additional Service pursuant to the Registry Services Evaluation Policy at http://www.icann.org/en/registries/rsep/rsep.html, as such policy may be amended from time to time (the "RSEP"). Registry Operator may offer Additional Services only with the written approval of ICANN. In its reasonable discretion, ICANN may require an amendment to this Agreement reflecting the provision of any Additional Service which is approved pursuant to the RSEP.

2.2   Compliance with Consensus Policies and Temporary Policies. Registry Operator shall comply with and implement all Consensus Policies and Temporary Policies found at <http://www.icann.org/general/consensus-policies.htm>, as of the Effective Date and as may in the future be developed and adopted in accordance with ICANN's Bylaws, provided such future Consensus Polices and Temporary Policies are adopted in accordance with the procedure and relate to those topics and subject to those limitations set forth at [*see specification 1*]*.

2.3   Data Escrow. Registry Operator shall comply with the registry data escrow procedures posted at [*see specification 2*]*.

2.4   Monthly Reporting. Within twenty (20) calendar days following the end of each calendar month, Registry Operator shall deliver to ICANN reports in the format posted at [*see specification 3*]*.

2.5   Publication of Registration Data. Registry Operator shall provide public access to registration data in accordance with the specification posted at [*see specification 4*]*.

2.6   Reserved Names. Except to the extent that ICANN otherwise expressly authorizes in writing, Registry Operator shall reserve from initial (i.e. other than renewal) registration all character strings that appear on the Schedule of Reserved Names posted at [see specification 5]*. Registry Operator may establish policies concerning the reservation or blocking of additional character strings within the TLD at its discretion. If Registry Operator is the registrant for any domain names in the Registry TLD (other than the Second-Level Reservations for Registry Operations from Specification 5), such registrations must be through an ICANN accredited registrar. Any such registrations will be considered Transactions (as defined in Section 6.1) for purposes of calculating the Registry-Level Transaction Fee to be paid to ICANN by Registry Operator pursuant to Section 6.1.

2.7   Functional and Performance Specifications. Functional and Performance Specifications for operation of the TLD will be as set forth at [*see specification 6*]*. Registry Operator shall comply with such Functional and Performance Specifications and, for a period of at least one year, shall keep technical and operational records sufficient to evidence compliance with such specifications.

---

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

2.8   **Protection of Legal Rights of Third Parties.** Registry Operator must specify, and comply with, a process and procedures for launch of the TLD and initial registration-related and ongoing protection of the legal rights of third parties, which shall at a minimum include those provisions set forth at [*see specification 7*]*. Any changes or modifications to such process and procedures following the Effective Date must be approved in advance by ICANN in writing.

2.9   **Use of Registrars**. Registry Operator must use only ICANN accredited registrars in registering domain names. Registry Operator must provide non-discriminatory access to registry services to all ICANN accredited registrars that enter into and are in compliance with Registry Operator's registry-registrar agreement for the TLD. Registry Operator must use a uniform agreement with all registrars authorized to register names in the TLD, which may be revised by Registry Operator from time to time, provided however, that any such revisions must be approved in advance by ICANN.

[There are four options for community discussion and consideration with respect to registry/registrar separation:

(a)   No cross-ownership restrictions except where there is market power and/or registry price caps (regulation needs, if any, left to regulating authorities)

(b)   No cross-ownership restrictions for new registries, existing restrictions for existing registries.

(c)   Limited lifting with enhanced structural separation:

(i)   The registrar cannot sell names in the co-owned registry, or

(ii)   The registrar can sell a very limited number of names in the co-owned registry.

(d)   Complete restrictions:

(i)   Registries cannot have ownership percentages in registrars, and vice versa.

(ii)   Registrars prohibited from providing back-end services (this might be accompanied by reciprocal restrictions, i.e., that registries cannot provide back-end services for other registries and registries cannot own resellers).]

2.10   **Pricing for Registry Services.** Except as set forth in this Section 2.10, Registry Operator shall provide each ICANN accredited registrar that has executed Registry Operator's registry-registrar agreement advance notice of any price increase [(net of refunds, rebates, discounts, product tying or other programs)] of no less than thirty (30) calendar days with respect to initial domain name registrations and one hundred eighty (180) calendar days with respect to renewal of domain name registrations, and shall offer registrars the option to obtain domain name registration renewals at the current price (i.e. the price in place prior to any noticed increase) for periods of one to ten years at the discretion of the registrar, but no greater than ten years. Notwithstanding the foregoing, with respect to renewal of domain name registrations, Registry Operator need only provide thirty (30) calendar days notice of any price increase if the resulting price is less than or equal to a price for which Registry Operator provided notice within that past twelve (12) months, and need not provide any notice of any price increase for the imposition of the Variable Registry-Level Fee set forth in Section 6.3. [Registry

---

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

Operator shall offer all domain registration renewals at the same price, unless the registrant agrees to a higher price at the time of the initial registration of the domain name following clear and conspicuous disclosure of such renewal price by Registry Operator.] Registry Operator shall provide public query-based DNS lookup service for the TLD at its sole expense.

2.11 **Contractual and Operational Compliance Audits.** ICANN may from time to time (not to exceed once per calendar quarter) conduct contractual compliance audits to assess compliance by Registry Operator with its covenants contained in Section 2 of this Agreement. Such audits shall be tailored to achieve the purpose of assessing compliance, and ICANN shall give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN. As part of such audit and upon request by ICANN, Registry Operator shall timely provide all responsive documents, data and any other information necessary to demonstrate Registry Operator's compliance with this Agreement. Upon no less than five (5) calendar days notice (unless otherwise agreed to by Registry Operator), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registry Operator with its covenants contained in Section 2 of this Agreement. Any such audit will be at ICANN's expense, unless such audit is related to a discrepancy in the fees paid by Registry Operator hereunder in excess of 5% to ICANN's detriment. In the latter event, Registry Operator shall reimburse ICANN for all reasonable costs and expenses associated with such audit, which reimbursement will be paid together with the next Registry-Level Fee payment due following the date of transmittal of the cost statement for such audit.

2.12 **Continued Operations Instrument.** Registry operator shall comply with the terms and conditions relating to the Continued Operations Instrument set forth at [*see specification 8*].

2.13 *[Note: For Community-Based TLDs Only]* **Obligations of Registry Operator to TLD Community.** Registry Operator shall establish registration policies in conformity with the application submitted with respect to the TLD for: (i) naming conventions within the TLD, (ii) requirements for registration by members of the TLD community, and (iii) use of registered domain names in conformity with the stated purpose of the community-based TLD. Registry Operator shall operate the TLD in a manner that allows the TLD community to discuss and participate in the development and modification of policies and practices for the TLD. Registry Operator shall establish procedures for the enforcement of registration policies for the TLD, and resolution of disputes concerning compliance with TLD registration policies, and shall enforce such registration policies. Registry Operator agrees to be bound by the Registry Restrictions Dispute Resolution Procedure as set forth at [*insert applicable URL*] with respect to disputes arising pursuant to this Section 2.13.]

ARTICLE 3.

COVENANTS OF ICANN

ICANN covenants and agrees with Registry Operator as follows:

3.1 **Open and Transparent.** Consistent with ICANN's expressed mission and core values, ICANN shall operate in an open and transparent manner.

3.2 **Equitable Treatment.** ICANN shall not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and shall not single out Registry Operator for disparate treatment unless justified by substantial and reasonable cause.

---

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

3.3 **TLD Nameservers.** ICANN will use commercially reasonable efforts to ensure that any changes to the TLD nameserver designations submitted to ICANN by Registry Operator (in a format and with required technical elements specified by ICANN at http://www.iana.org/domains/root/ will be implemented by ICANN within seven (7) calendar days or as promptly as feasible following technical verifications. To the extent that ICANN is authorized to set policy with regard to an authoritative root server system, ICANN will ensure that the authoritative root will point to the top-level domain nameservers designated by Registry Operator for the TLD throughout the Term of this Agreement, unless earlier terminated pursuant to Section 4.3 or 4.4.

3.4 **Root-zone Information Publication.** ICANN's publication of root-zone contact information for the Registry TLD will include Registry Operator and its administrative and technical contacts. Any request to modify the contact information for the Registry Operator must be made in the format specified from time to time by ICANN at http://www.iana.org/domains/root/.

ARTICLE 4.

TERM AND TERMINATION

4.1 **Term.** The term of this Agreement will be ten years from the Effective Date (as such term may be extended pursuant to Section 4.2, the "Term").

4.2 **Renewal.** This Agreement will be renewed for successive periods of ten years upon the expiration of the initial Term set forth in Section 4.1 and each successive Term, unless:

(a) Following notice by ICANN to Registry Operator of a fundamental and material breach of Registry Operator's covenants set forth in Article 2 or default of its payment obligations under Article 6 of this Agreement, which notice shall include with specificity the details of the alleged breach or default and such breach or default has not been cured within thirty (30) calendar days of such notice, (i) an arbitrator or court has finally determined that Registry Operator has been in fundamental and material breach of such covenant(s) or in default of its payment obligations, and (ii) Registry Operator has failed to comply with such determination and cure such breach or default within ten (10) calendar days or such other time period as may be determined by the arbitrator or court; or

(b) During the then current Term, Registry Operator shall have been found by an arbitrator (pursuant to Section 5.2 of this Agreement) on at least three (3) separate occasions to have been in fundamental and material breach (whether or not cured) of Registry Operator's covenants set forth in Article 2 or default of its payment obligations under Article 6 of this Agreement.

(c) Upon the occurrence of the events set forth in Section 4.2(a) or (b), the Agreement shall terminate at the expiration of the then current Term.

4.3 **Termination by ICANN.**

(a) ICANN may terminate this Agreement if: (i) Registry Operator fails to cure any fundamental and material breach of Registry Operator's covenants set forth in Article 2 or default of its payment obligations set forth in Article 6 of this Agreement, each within thirty (30) calendar days after ICANN gives Registry Operator notice of such breach or default, which notice will include with specificity the details of the alleged breach or default, (ii) an arbitrator or court has finally determined that Registry Operator is in fundamental and material breach of such covenant(s) or in default of its payment obligations, and (iii) Registry Operator fails to comply with such determination and cure such breach or

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

default within ten (10) calendar days or such other time period as may be determined by the arbitrator or court.

(b)   ICANN may, upon notice to Registry Operator, terminate this Agreement, if Registry Operator fails to complete all testing and procedures necessary for delegation of the TLD into the root zone within 12 months of the Effective Date. Registry Operator may request an extension for up to additional 12 months for delegation if it can demonstrate, to ICANN's reasonable satisfaction, that Registry Operator is working diligently and in good faith toward successfully completing the steps necessary for delegation of the TLD. Any fees paid by Registry Operator to ICANN prior to such termination date shall be retained by ICANN in full.

(c)   ICANN may, upon notice to Registry Operator, terminate this agreement if Registry Operator fails to cure a breach of Registry Operator's obligations set forth in Section 2.12 of this Agreement within thirty (30) calendar days of delivery of notice of such breach by ICANN, or if the Continued Operations Instrument is not in effect for greater than sixty (60) consecutive calendar days at any time following the Effective Date.

4.4   Termination by Registry Operator.

(a)   Registry Operator may terminate this Agreement upon notice to ICANN if, (i) ICANN fails to cure any fundamental and material breach of ICANN's covenants set forth in Article 3, within thirty (30) calendar days after Registry Operator gives ICANN notice of such breach, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court has finally determined that ICANN is in fundamental and material breach, and (iii) ICANN fails to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court.

(b)   Registry Operator may terminate this Agreement upon notice to ICANN if, (i) within the notice period provided for in Section 7.2(d), Registry Operator provides ICANN notice of its objection to a proposed material amendment of this Agreement pursuant to Article 7, which notice will include with specificity the details of such objection, and (ii) such amendment thereafter becomes effective in the form objected to by Registry Operator; provided, however, that Registry Operator may only terminate this Agreement pursuant to this Section 4.4(b) if the required notice of termination has been provided to ICANN within thirty (30) calendar days following the effective date of such amendment; provided, further, that the termination of this Agreement pursuant to this Section 4.4(b) shall be effective on the date that is the one hundred twenty (120) calendar day following the date upon which Registry Operator delivered the notice of termination to ICANN.

(c)   Registry Operator may terminate this Agreement for any reason upon one hundred eighty (180) calendar day advance notice to ICANN.

4.5   Transition of Registry upon Termination of Agreement. Upon expiration of the Term and any termination of this Agreement, Registry Operator shall agree to provide ICANN or any successor registry authority that may be designated by ICANN for the TLD with all data (including that data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by ICANN or such successor registry authority. After consultation with Registry Operator, ICANN shall determine whether or not to transition operation of the TLD to a successor registry authority in its sole discretion and in conformance with the ICANN gTLD Registry Continuity Plan, dated April 25, 2009, as the same may be amended from time to time. In addition, ICANN or its designee shall retain and may enforce its rights under the

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

7

Continued Operations Instrument and Alternative Instrument, as applicable, regardless of the reason for termination or expiration of this Agreement.

4.6 Survival. Expiration or termination of this Agreement shall not relieve the parties of any obligation or breach of this Agreement accruing prior to such expiration or termination, including, without limitation, all accrued payment obligations arising under Article 6. In addition Article 5 and Article 8, Section 2.12, Section 4.5, and this Section 4.6 shall survive the expiration or termination of this Agreement.

ARTICLE 5.

DISPUTE RESOLUTION

5.1 Cooperative Engagement. Before either party may initiate arbitration pursuant to Section 5.2 below, ICANN and Registry Operator, following initiation of communications by either party, must attempt to resolve the dispute by engaging in good faith discussion over a period of at least fifteen (15) calendar days.

5.2 Arbitration. Disputes arising under or in connection with this Agreement, including requests for specific performance, will be resolved through binding arbitration conducted pursuant to the rules of the International Court of Arbitration of the International Chamber of Commerce ("ICC"). The arbitration will be conducted in the English language in front of a single arbitrator and will occur in Los Angeles County, California, USA. The prevailing party in the arbitration will have the right to recover its costs and reasonable attorneys' fees, which the arbitrator shall include in its awards. In any proceeding, ICANN may request the appointed arbitrator award punitive or exemplary damages, or operational sanctions (including without limitation an order temporarily restricting Registry Operator's right to sell new registrations) in the event the arbitrator determines that Registry Operator has been repeatedly and willfully in fundamental and material breach of its obligations set forth in Article 2, Article 6 and Section 5.4 of this Agreement. In any litigation involving ICANN concerning this Agreement, jurisdiction and exclusive venue for such litigation will be in a court located in Los Angeles County, California, USA; however, the parties will also have the right to enforce a judgment of such a court in any court of competent jurisdiction.

5.3 Limitation of Liability. ICANN's aggregate monetary liability for violations of this Agreement will not exceed the amount of Registry-Level Fees paid by Registry Operator to ICANN within the preceding twelve-month period pursuant to this Agreement (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any). Registry Operator's aggregate monetary liability to ICANN for violations of this Agreement will be limited to the amount of fees paid to ICANN during the preceding twelve-month period (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any), and punitive and exemplary damages, if any, awarded in accordance with Section 5.2. In no event shall either party be liable for special, punitive, exemplary or consequential damages arising out of or in connection with this Agreement or the performance or nonperformance of obligations undertaken in this Agreement, except as provided in Section 5.2.

5.4 Specific Performance. Registry Operator and ICANN agree that irreparable damage could occur if any of the provisions of this Agreement was not performed in accordance with its specific terms. Accordingly, the parties agree that they each shall be entitled to seek from the arbitrator specific performance of the terms of this Agreement (in addition to any other remedy to which each party is entitled).

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

ARTICLE 6.

FEES

      6.1   **Registry-Level Fees.** Registry Operator shall pay ICANN a Registry-Level Fee equal to (i) the Registry Fixed Fee of US$6,250 per calendar quarter and (ii) the Registry-Level Transaction Fee. The Registry-Level Transaction Fee will be equal to the number of annual increments of an initial or renewal domain name registration (at one or more levels, and including renewals associated with transfers from one ICANN-accredited registrar to another, each a "Transaction"), during the applicable calendar quarter multiplied by US$0.25, provided, however that the Registry-Level Transaction Fee shall not apply until and unless more than 50,000 domain names are registered in the TLD and shall apply thereafter to each Transaction. Registry Operator shall pay the Registry-Level Fees on a quarterly basis comprised of four equal payments by the 20th day following the end of each calendar quarter (i.e., on April 20, July 20, October 20 and January 20 for the calendar quarters ending March 31, June 30, September 30 and December 31) of the year to an account designated by ICANN.

      6.2   **Cost Recovery for RSTEP.** Requests by Registry Operator for the approval of Additional Services pursuant to Section 2.1 may be referred by ICANN to the Registry Services Technical Evaluation Panel ("RSTEP") pursuant to that process at http://www.icann.org/en/registries/rsep/. In the event that such requests are referred to RSTEP, Registry Operator shall remit to ICANN the invoiced cost of the RSTEP review within ten (10) business days of receipt of a copy of the RSTEP invoice from ICANN, unless ICANN determines, in its sole and absolute discretion, to pay all or any portion of the invoiced cost of such RSTEP review.

      6.3   **Variable Registry-Level Fee.**

          (a)   If the ICANN accredited registrars (as a group) do not approve pursuant to the terms of their registrar accreditation agreements with ICANN the variable accreditation fees established by the ICANN Board of Directors for any ICANN fiscal year, upon delivery of notice from ICANN, Registry Operator shall pay to ICANN a Variable Registry-Level Fee, which shall be paid on a fiscal quarter basis, and shall accrue as of the beginning of the first fiscal quarter of such ICANN fiscal year. The fee will be calculated and invoiced by ICANN on a quarterly basis, and shall be paid by Registry Operator within sixty (60) calendar days with respect to the first quarter of such ICANN fiscal year and within twenty (20) calendar days with respect to each remaining quarter of such ICANN fiscal year, of receipt of the invoiced amount by ICANN. The Registry Operator may invoice and collect the Variable Registry-Level Fees from the registrars who are party to a Registry-Registrar Agreement with Registry Operator, provided that the fees shall be invoiced to all ICANN accredited registrars if invoiced to any. The Variable Registry-Level Fee, if collectible by ICANN, shall be an obligation of Registry Operator and shall be due and payable as provided in this Section 6.3 irrespective of Registry Operator's ability to seek and obtain reimbursement of such fee from registrars. In the event ICANN later collects variable accreditation fees for which Registry Operator has paid ICANN a Variable Registry-Level Fee, ICANN shall reimburse the Registry Operator an appropriate amount of the Variable Registry-Level Fee, as reasonably determined by ICANN. If the ICANN accredited registrars (as a group) do approve pursuant to the terms of their registrar accreditation agreements with ICANN the variable accreditation fees established by the ICANN Board of Directors for a fiscal year, ICANN shall not be entitled to a Variable-Level Fee hereunder for such fiscal year, irrespective of whether the ICANN accredited registrars comply with their payment obligations to ICANN during such fiscal year.

          (b)   The amount of the Variable Registry-Level Fee will be specified for each registrar, and may include both a per-registrar component and a transactional component. The per-

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

registrar component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year. The transactional component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year but shall not exceed US$0.25 per domain name registration (including renewals associated with transfers from one ICANN-accredited registrar to another) per year.

6.4   Adjustments to Fees. Notwithstanding any of the fee limitations set forth in this Article 6, commencing upon the expiration of the first year of this Agreement, and upon the expiration of each year thereafter during the Term, the then current fees set forth in Section 6.1 and Section 6.3 may be increased, at ICANN's discretion, by a percentage equal to the percentage increase, if any, in (i) the Consumer Price Index for All Urban Consumers, U.S. City Average (1982-1984 = 100) published by the United States Department of Labor, Bureau of Labor Statistics, or any successor index (the "CPI") for the month which is one (1) month prior to the commencement of the applicable year, over (ii) the CPI published for the month which is one (1) month prior to the commencement of the immediately prior year. In the event of any such increase, ICANN shall provide notice to Registry Operator specifying the amount of such increase. Any fee increase under this Section 6.4 shall be effective as of the first day of the year in which the above calculation is made.

6.5   Additional Fee on Late Payments. For any payments thirty (30) calendar days or more overdue under this Agreement, Registry Operator shall pay an additional fee on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law.

ARTICLE 7.

AMENDMENTS

7.1   Amendment of Terms and Specifications. During the term of this Agreement, Article 2 (including the specifications incorporated into this Agreement pursuant to Article 2), Article 6 and Article 8 may be amended by ICANN in accordance with changing standards, policies and requirements pursuant to the process set forth in this Article 7; provided, however, that (i) ICANN may not utilize this Article 7 to increase the amount of fees payable hereunder unless ICANN demonstrates a financial need for any such increase, (ii) no amendment shall be applied retrospectively, and (iii) ICANN may not utilize this Article 7 to amend Section 2.1, Section 2.2 or the process set forth at [*see specification 1*] for adoption and implementation of new or modified Consensus Policies or Temporary Policies.

7.2   Process for Changes. The process for any amendment to this Agreement pursuant to Section 7.1 shall be as follows:

(a)   Prior to formally proposing any amendment, ICANN will provide an opportunity of no less than thirty (30) calendar days for consultation with and consideration of input from all registry operators that would be subject to such amendment;

(b)   Following such consultation and consideration, ICANN will publicly post on its website for no less than thirty (30) calendar days formal notice of any proposed amendment to this Agreement, including the text of the amendment (including any amendment to the specifications incorporated into this Agreement), during which Registry Operator may submit comments to the amendment;

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

10

(c)   Following such public notice period and approval of the amendment by the ICANN Board of Directors, ICANN shall provide Registry Operator notice of the final terms of the amendment (including any amendment to the specifications incorporated into this Agreement) at least ninety (90) calendar days prior to the effectiveness thereof by the posting of a notice of effectiveness on ICANN's web site;

(d)   From the date of such public notice of the approved amendment, Registry Operator shall have sixty (60) calendar days to provide notice to ICANN of its disapproval of such amendment;

(e)   If, within such sixty (60) calendar day period, the registry operators of a majority of the top-level domains subject to the amendment (i.e. Registry Operator and any other registry operator party to a registry agreement with ICANN containing a provision similar to this Article 7) provide notice to ICANN of their disapproval of the amendment, it shall be deemed disapproved by the affected registry operators; and

(f)   In the event that the amendment is disapproved by the affected registry operators pursuant to the process set forth in clause (e) above, the ICANN Board of Directors by a two-thirds vote shall have thirty (30) calendar days to override such disapproval if: (i) in the case of any amendment relating to the fees payable to ICANN hereunder, the amendment is justified by a financial need of ICANN and (ii) in the case of any other amendment, the amendment is justified by a substantial and compelling need related to the Security or Stability (as such terms are defined in Section 8.3) of the Internet or the Domain Name System, in which case, the proposed amendment shall be effective immediately upon expiration of such thirty (30) calendar day period. If the ICANN Board of Directors does not override such disapproval, the proposed amendment shall have no force or effect.

ARTICLE 8.

MISCELLANEOUS

8.1   Indemnification of ICANN.

(a)   Registry Operator shall indemnify and defend ICANN and its directors, officers, employees, and agents (collectively, "Indemnitees") from and against any and all third-party claims, damages, liabilities, costs, and expenses, including legal fees and expenses, arising out of or relating to Registry Operator's operation of the registry for the TLD or Registry Operator's provision of Registry Services; provided that Registry Operator shall not be obligated to indemnify or defend any Indemnitee to the extent the claim, damage, liability, cost or expense arose due to a breach by ICANN of any obligation contained in this Agreement or any willful misconduct by ICANN. This section will not apply to any request for attorneys' fees in connection with any litigation or arbitration between or among the parties. This section shall not be deemed to require Registry Operator to reimburse or otherwise indemnify ICANN for costs associated with the negotiation or execution of this Agreement, or with monitoring or management of the parties' respective obligations hereunder. Further, this Section shall not apply to any request for attorney's fees in connection with any litigation or arbitration between or among the parties, which shall be governed by Article 5 or otherwise awarded by a court or arbitrator.

(b)   For any claims by ICANN for indemnification whereby multiple registry operators (including Registry Operator) have engaged in the same actions or omissions that gave rise to the claim, Registry Operator's aggregate liability to indemnify ICANN with respect to such claim shall be limited to a percentage of ICANN's total claim, calculated by dividing the number of total domain names

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

11

under registration with Registry Operator within the TLD (which names under registration shall be calculated consistently with Article 6 hereof for any applicable quarter) by the total number of domain names under registration within all top level domains for which the registry operators thereof that are engaging in the same acts or omissions giving rise to such claim. For the purposes of reducing Registry Operator's liability under Section 8.1(a) pursuant to this Section 8.1(b), Registry Operator shall have the burden of identifying the other registry operators that are engaged in the same actions or omissions that gave rise to the claim, and demonstrating, to ICANN's reasonable satisfaction, such other registry operators' culpability for such actions or omissions. For the avoidance of doubt, in the event that a registry operator is engaged in the same acts or omissions giving rise to the claims, but such registry operator(s) do not have the same or similar indemnification obligations to ICANN as set forth in Section 8.1(a) above, the number of domains under management by such registry operator(s) shall nonetheless be included in the calculation in the preceding sentence.

8.2 **Indemnification Procedures.** If any third-party claim is commenced that is indemnified under Section 8.1 above, ICANN shall provide notice thereof to Registry Operator as promptly as practicable. Registry Operator shall be entitled, if it so elects, in a notice promptly delivered to ICANN, to immediately take control of the defense and investigation of such claim and to employ and engage attorneys reasonably acceptable to ICANN to handle and defend the same, at Registry Operator's sole cost and expense, provided that in all events ICANN will be entitled to control at its sole cost and expense the litigation of issues concerning the validity or interpretation of ICANN policies or conduct. ICANN shall cooperate, at Registry Operator's cost and expense, in all reasonable respects with Registry Operator and its attorneys in the investigation, trial, and defense of such claim and any appeal arising therefrom, and may, at its own cost and expense, participate, through its attorneys or otherwise, in such investigation, trial and defense of such claim and any appeal arising therefrom. No settlement of a claim that involves a remedy affecting ICANN other than the payment of money in an amount that is fully indemnified by Registry Operator will be entered into without the consent of ICANN. If Registry Operator does not assume full control over the defense of a claim subject to such defense in accordance with this Section 8.2, ICANN will have the right to defend the claim in such manner as it may deem appropriate, at the cost and expense of Registry Operator.

8.3 **Defined Terms.** For purposes of this Agreement, Security and Stability shall be defined as follows:

(a) For the purposes of this Agreement, an effect on "Security" shall mean (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.

(b) For purposes of this Agreement, an effect on "Stability" shall refer to (1) lack of compliance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice Requests for Comments ("RFCs") sponsored by the Internet Engineering Task Force; or (2) the creation of 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 and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice RFCs, and relying on Registry Operator's delegated information or provisioning of services.

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

8.4 **No Offset.** All payments due under this Agreement will be made in a timely manner throughout the Term and notwithstanding the pendency of any dispute (monetary or otherwise) between Registry Operator and ICANN.

8.5 **Change in Control; Assignment and Subcontracting.** Neither party may assign this Agreement without the prior written approval of the other party, which approval will not be unreasonably withheld. Notwithstanding the foregoing, ICANN may assign this Agreement in conjunction with a reorganization or re-incorporation of ICANN to another nonprofit corporation or similar entity organized for the same or substantially the same purposes. Registry Operator must provide no less than thirty (30) calendar days advance notice to ICANN of any material subcontracting arrangements, and any agreement to subcontract portions of the operations of the TLD must mandate compliance with all covenants, obligations and agreements by Registry Operator hereunder. Registry Operator will provide no less than ten (10) calendar days advance notice to ICANN prior to the consummation of any transaction anticipated to result in a direct or indirect change of ownership or control of Registry Operator. Such change of ownership or control notification shall include a statement that affirms that the ultimate parent entity of the party acquiring such ownership or control meets the ICANN-adopted specification or policy on registry operator criteria then in effect, and affirms that Registry Operator is in compliance with its obligations under this Agreement. Within thirty (30) calendar days of such notification, ICANN may request additional information from Registry Operator establishing compliance with this Agreement, in which case Registry Operator must supply the requested information within fifteen (15) calendar days.

8.6 **Amendments and Waivers.** Except as set forth in Article 7, no amendment, supplement, or modification of this Agreement or any provision hereof will be binding unless executed in writing by both parties. Irrespective of the provisions of Article 7, ICANN and Registry Operator may at any time and from time to time enter into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement will be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to enforce any of the provisions hereof will be deemed or will constitute a waiver of any other provision hereof, nor will any such waiver constitute a continuing waiver unless otherwise expressly provided.

8.7 **No Third-Party Beneficiaries.** This Agreement will not be construed to create any obligation by either ICANN or Registry Operator to any non-party to this Agreement, including any registrar or registered name holder.

8.8 **General Notices.** Except for notices pursuant to Article 7, all notices to be given under or in relation to this Agreement will be given either (i) in writing at the address of the appropriate party as set forth below or (ii) via facsimile or electronic mail as provided below, unless that party has given a notice of change of postal or email address, or facsimile number, as provided in this agreement. All notices under Article 7 shall be given by both posting of the applicable information on ICANN's web site and transmission of such information to Registry Operator by electronic mail. Any change in the contact information for notice below will be given by the party within thirty (30) calendar days of such change. Notices, designations, determinations, and specifications made under this Agreement will be in the English language. Other than notices under Article 7, any notice required by this Agreement will be deemed to have been properly given (i) if in paper form, when delivered in person or via courier service with confirmation of receipt or (ii) if via facsimile or by electronic mail, upon confirmation of receipt by the recipient's facsimile machine or email server, provided, that such notice via facsimile or electronic mail shall be followed by a copy sent by regular postal mail service within two (2) business days. Any notice required by Article 7 will be deemed to have been given when electronically posted on ICANN's website and upon confirmation of receipt by the email server. In the event other means of notice become

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

13

practically achievable, such as notice via a secure website, the parties will work together to implement such notice means under this Agreement.

> If to ICANN, addressed to:
> Internet Corporation for Assigned Names and Numbers
> 4676 Admiralty Way, Suite 330
> Marina Del Rey, California 90292
> Telephone: 1-310-823-9358
> Facsimile: 1-310-823-8649
> Attention: President and CEO
> With a Required Copy to: General Counsel
> Email: (As specified from time to time.)
>
> If to Registry Operator, addressed to:
> [_____]
> [_____]
> [_____]
> Telephone:
> Facsimile:
> Attention:
> With a Required Copy to:
> Email: (As specified from time to time.)

8.9 **Entire Agreement.** This Agreement (including those specifications and documents incorporated by reference to URL locations which form a part of it) constitutes the entire agreement of the parties hereto pertaining to the operation of the TLD and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

8.10 **English Language Controls.** Notwithstanding any translated version of this Agreement and/or specifications that may be provided to Registry Operator, the English language version of this Agreement and all referenced specifications are the official versions that bind the parties hereto. In the event of any conflict or discrepancy between any translated version of this Agreement and the English language version, the English language version controls. Notices, designations, determinations, and specifications made under this Agreement shall be in the English language.

<p align="center">* * * * *</p>

<p align="center">* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.</p>

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By: _____

[_____]

President and CEO

Date:

[Registry Operator]

By: _____

[_____]

[_____]

Date:

* Final text will be posted on ICANN website; agreement reference to be replaced by hyperlink.

EXHIBIT A

<u>Approved Services</u>

SPECIFICATION 1

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. **Consensus Policies.**

1.1. "***Consensus Policies***" are those policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this document. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with the process set forth therein.

1.2. Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including the operators of gTLDs. Consensus Policies shall relate to one or more of the following:

1.2.1. issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or Domain Name System ("DNS");

1.2.2. functional and performance specifications for the provision of registry services;

1.2.3. Security and stability of the registry database for the TLD;

1.2.4. registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars; or

1.2.5. resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names).

1.3. Such categories of issues referred to in Section 1.2 shall include, without limitation:

1.3.1. principles for allocation of registered names in the TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);

1.3.2. prohibitions on warehousing of or speculation in domain names by registries or registrars;

1.3.3. reservation of registered names in the TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration); and

1.3.4. maintenance of and access to accurate and up-to-date information concerning domain name registrations; and procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility for serving registered domain names in a TLD affected by such a suspension or termination.

1.4. In addition to the other limitations on Consensus Policies, they shall not:

1.4.1. prescribe or limit the price of registry services;

1.4.2. modify the terms or conditions for the renewal or termination of the Registry Agreement;

1.4.3. modify the limitations on Temporary Policies (defined below) or Consensus Policies;

1.4.4. modify the provisions in the registry agreement regarding fees paid by Registry Operator to ICANN; or

1.4.5. modify ICANN's obligations to ensure equitable treatment of registry operators and act in an open and transparent manner.

2. **Temporary Policies.** Registry Operator shall comply with and implement all specifications or policies established by the Board on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of registry services or the DNS ("*Temporary Policies*").

   2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.

      2.1.1. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.

      2.1.2. If the period of time for which the Temporary Policy is adopted exceeds 90 days, the Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed one year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one year period expires or, if during such one year period, the Temporary Policy does not become a Consensus Policy and is not reaffirmed by the Board, Registry Operator shall no longer be required to comply with or implement such Temporary Policy.

3. **Notice and Conflicts.** Registry Operator shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between registry services and Consensus Policies or any Temporary Policy, the Consensus Polices or Temporary Policy shall control, but only with respect to subject matter in conflict.

SPECIFICATION 2
DATA ESCROW REQUIREMENTS
NOTE: THIS INTERIM DRAFT SPECIFICATION IS UNDER DEVELOPMENT BY ICANN AND REGISTRY TECHNICAL TEAMS.

Registry Operator will engage an independent entity to act as data escrow agent ("***Escrow Agent***") for the provision of data escrow services related to the Registry Agreement. The following Technical Specifications set forth in Part A, and Legal Requirements set forth in Part B, will be included in any data escrow agreement between Registry Operator and the Escrow Agent, under which ICANN must be named a third-party beneficiary. In addition to the following requirements, the data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms provided below.

PART A – TECHNICAL SPECIFICATIONS

1.   <u>**Deposits**</u>. <u>Deposits</u> can be of two kinds: Full Deposits or Incremental Deposits.

    1.1 "**Full Deposit**" means the Registry Data that reflects the current and complete Registry Database and will consist of data that reflects the state of the registry as of 0000 UTC on each Sunday. Pending transactions at that time (i.e. transactions that have not been committed to the Registry Database) will not be reflected in the Full Deposit.

    1.2 "**Incremental Deposit**" means data that reflects all transactions involving the database that were not reflected in the last previous Full Deposit or Incremental Deposit, as the case may be. Each incremental file will contain all database transactions since the previous Deposit was completed as of 0000 UTC. Incremental deposits, where required, must include complete Escrow Records as specified below that were not included or changed since the most recent full or incremental deposit (i.e., newly added or modified names).

2.   <u>**Procedure for Deposits**</u>. Each formatted Full Deposit and Incremental Deposit must be processed and delivered in encrypted form to Escrow Agent. The formatted, encrypted and signed Deposit file(s) must be sent, by authenticated, secure file transfer, to Escrow Agent's server within the specified time window, see **PART B – LEGAL REQUIREMENTS**.

3.   <u>**Schedule for Deposits**</u>. Registry operators are obligated to submit a set of escrow files on a daily basis as follows:

    3.1 Once a week, a Full Deposit of the entire set of objects in the registry must be submitted. Each of these files will be marked with the "full" type.

    3.2 The other six days of the week, an Incremental Deposit must be submitted including objects that have been created, deleted or updated. Each of these files will be marked with the "inc" type.

    3.3 Each incremental submission must cover the time period since the generation of the previous submission.

    3.4 Although we expect this to be an exception, it is permissible to have some overlap between Incremental Deposits.

4.   <u>**Escrow Format Specification.**</u>

    4.1 **File Naming Conventions.** Files shall be named according to the following convention:
        <gTLD>_<YYYY-MM-DD>_<FILE>_<type>_<comp>_<encrypt>_S<#>_R<rev>.<ext> where:

    4.1.1   <gTLD> is replaced with the gTLD name; in case of an IDN-TLD, the ASCII-label must be used;

4.1.2   <YYYY-MM-DD> is replaced by the date corresponding to the time used as a timeline watermark for the transactions; i.e. for the Full Deposit corresponding to 2009-08-02T00:00Z, the string to be used would be "2009-08-02";

4.1.3   <FILE> is replaced with the file type as indicated in 4.8 below;

4.1.4   <type> is replaced by:
     (1) "full", if the data represents a full deposit;
     (2) "inc", if the data represents an incremental deposit;

4.1.5   <comp> is replaced by the name of compression algorithm used, see section 4.10:

4.1.6   <encrypt> is replaced by the corresponding encryption algorithm used, see section 4.10:

4.1.7   <#> is replaced by the position of the file in a series of files, beginning with "1"; in case of a lone file, this must be replaced by "1".

4.1.8   <rev> is replaced by the number of revision (or resend) of the file beginning with "0":

4.1.9   <ext> is replaced by "data" if the file contains actual data (may be compressed and/or encrypted) or "sig" for the digital signature file of the corresponding data file.

4.2   **Object Handles.** For each of the object types (domains, contacts, name servers, DNSSEC delegation signer records, and registrars), an ID or "handle" will be used to permit compactly referencing objects from other files.

4.2.1   These handles may be represented as alphanumeric values, offering maximum flexibility.

4.2.2   Registry operator may use the domain name as the domain handle.

4.3   **Dates.** Numerous fields indicate "dates", such as the creation and expiry dates for domains. These fields should contain timestamps indicating the date and time in a format and time zone that is consistent across all such fields in the escrow deposit. Timestamps should be presented relative to UTC consistent with the date/time handling used in EPP RFC 4930 [1].

4.4   **CSV Format.** Escrow data shall be compiled into CSV text files, as described in RFC 4180 [5]. The character encoding for these files should be UTF-8. Once compressed and/or encrypted the data files shall be in binary form. Signature files shall never be compressed nor encrypted.

4.5   **Object Statuses.** RFC 4930 (EPP) and related RFCs, see [1], [2], [3], [4] indicate permissible status codes for various registry objects. Additionally the status "reserved" is allowed for domains; it is used to indicate a reserved name on behalf of the Registry or ICANN.

4.6   **Reserved Name Handling.** Registries typically have a set of names reserved on behalf of themselves or IANA. Reserved names must be included in the DOMAIN file, and have the special "reserved" status associated with them in the DOMSTATUS file to indicate that they are reserved.

4.7   **Variant Handling.** If Registry Operator offers IDNs, the variant table and registration policy must be deposited with the IANA IDN Practices Repository [9]. In some cases, for a particular name, there may be multiple "variants," where reservation of a domain name indicates reservation of one or more other names that are equivalent, in the language representation. Depending on implementation, there are several possible approaches for escrow, the Registry shall use the most appropriate to its needs:
     (1) Multiple name variants may be expressed in the registry, and presented in the DNS zone; each such name shall be stored in the DOMAIN and DOMIDN files, as described below.
     (2) It may suffice, in some cases, to store variants in the form shown above as the "DOMIDN" file, where variant names, in Unicode form, are associated with the "parent/canonical" domain name.

(3) There will be cases where there is an algorithm used to generate variant names, and where the number of variants would be impractical to store or to submit directly for escrow. In such cases, out of band documentation must provide details about variant generation algorithms. It may also be necessary to add an extension file to indicate, for domains having variant names, the algorithm and any other parameters used to compute variants.

4.8 **Detailed File Formats.**

For each object the order in which its fields are presented indicates the order in which they are expected to be in the respective record. The first line of all files must contain the field names.

4.8.1　**Domains.** Indicates a file type "DOMAIN"

The following fields shall be stored in the DOMAIN file:

(1) Domain Handle;

(2) Domain Name;

(3) Registrar Handle for the present sponsoring registrar;

(4) Creation Date;

(5) Registrar Handle for the initial sponsoring registrar;

(6) Expiry Date;

(7) Authinfo for the domain; and

4.8.2　**Internationalized Domain Names (IDNs).** In the case of internationalized domain names, the ASCII-compatible form (A-Label) of the IDN string shall be referenced in the domain name field (e.g. - "xn-11b5bs1di.tld"), not the Unicode label (U-Label).

The following fields shall be stored in the DOMIDN file:

(1) Domain Handle;

(2) Unicode Label/U-Label;

(3) Language Tag (based on ISO 639-1); and

(4) Script Tag (based on ISO 15924).

4.8.3　**Contacts.** Indicates a file type "CONTACT".

The following fields shall be stored in the CONTACT file:

(1) Contact Handle;

(2) Registrar Handle for the sponsoring registrar;

(3) Creation Date;

(4) Authinfo for the contact;

(5) Voice Telephone Number;

(6) Voice Telephone Extension;

(7) Fax Telephone Number;

(8) Fax Extension;

(9) Email Address.

(10)　　　Registrar Handle of the creator registrar;

(11)　　　Registrar Handle of the registrar who last updated the contact;

(12)　　　Last update Date;

(13)　　　Last transfer Date;

4.8.4 **Contacts' addresses.** Indicates a file type "CONADDR". Contains the addresses of the Contacts. Only two addresses per Contact are allowed provided they are of different types.
The following fields shall be stored in the CONADDR file:

(1) Contact Handle;
(2) Address type: int / loc; see RFC 4933 [4];
(3) Contact Name;
(4) Contact Organization;
(5) Postal Address 1;
(6) Postal Address 2;
(7) Postal Address 3;
(8) City;
(9) State/Province/Region;
(10)   Postal Code;
(11)   Country;

Notes for 4.8.3 and 4.8.4:
The following fields are ones where standards documents may be able to indicate requirements appropriate to validation. In particular, the EPP Contact Mapping [4] requires reference to other standards documents as follows:

Country
Country identifiers are represented using two character identifiers as specified in ISO 3166.

Telephone numbers
Telephone numbers (both voice and fax) are formatted based on structures defined in ITU standard E164a.

Email Address
Email address syntax is defined in RFC 2822.

4.8.5 **Name servers.** Indicates a file type "NAMESERVER".
The following fields shall be stored in the NAMESERVER file:

(1) Name server Handle;
(2) Name server Name;
(3) Creation Date; and
(4) Registrar Handle of sponsoring registrar.

4.8.6 **Name server IP Addresses.** Indicates a file type "NSIP"
The following fields shall be stored in the NSIP file:

(1) Name server Handle; and
(2) IP Address.

Notes. IP addresses must conform either to, RFC 791, for IPv4 addresses, or RFC 4291, for IPv6 addresses.

4.8.7 **Registrars.** Indicates a file type "REGISTRAR"
The following fields shall be stored in the REGISTRAR file:

(1) Registrar Handle;
(2) IANA ID for Registrar as per IANA Registrar IDs [8]; and
(3) Registrar Name;

4.8.8 **Domain/Status Associations.** Indicates a file type "DOMSTATUS"
The following fields shall be stored in the DOMSTATUS file:
(1) Domain Handle;
(2) Status Value, as per the earlier section on Object Statuses; and
(3) Reason Code.

4.8.9 **Contact/Status Associations.** Indicates a file type "CONSTATUS"
The following fields shall be stored in the CONSTATUS file:
(1) Contact Handle;
(2) Status Value, as per the earlier section on Object Statuses; and
(3) Reason Code.

4.8.10 **Name server/Status Associations.** Indicates a file type "NSSTATUS"
The following fields shall be stored in the NSSTATUS file:
(1) Name server Handle;
(2) Status Value, as per the earlier section on Object Statuses; and
(3) Reason Code.

4.8.11 **Domain/Contact Associations.** Indicates a file type "DOMCONTACT"
The following fields shall be stored in the DOMCONTACT file:
(1) Domain Handle;
(2) Contact Handle; and
(3) Contact Type.

Type Possible	Abbreviations
Registrant Contact	R, REG
Administrative Contact	A, ADMIN
Billing Contact	B, BILL
Technical Contact	T, TECH

4.8.12 **Domain / Name server Associations.** Indicates a file type "DOMNS"
The following fields shall be stored in the DOMNS file:
(1) Domain Handle; and
(2) Name server Handle.

4.8.13 **Domain Deletions.** Indicates a file type "DOMDEL." This file must be sent only for incremental escrow deposits (e.g. - file type "inc"); it indicates the list of domains that were in the previous deposit that have since been removed.
(1) Domain Name; and
(2) Deletion Date.

4.8.14 **Contact Deletions.** Indicates a file type "CONTDEL." This file must be sent only for incremental escrow deposits (e.g. - file type "inc"); it indicates the list of contacts that were in the previous deposit that have since been removed.
(1) Contact Handle; and
(2) Deletion Date.

4.8.15 **Name server Deletions.** Indicates a file type "NSDEL." This file must be sent only for incremental escrow deposits (e.g. file type "inc"); it indicates the list of name servers that were in the previous deposit, that have since been removed.

(1) Name server Name; and

(2) Deletion Date.

4.8.16 **Domain/DNSSEC Delegation Signer Record Associations.** Indicates a file type "DOMDS". Only the first five fields are mandatory, the rest may be left blank. These fields are related to those described in RFC 4310 [10].
The following fields shall be stored in the DSDEL file:

(1) Domain Handle;

(2) KeyTag;

(3) Algorithm;

(4) Digest Type;

(5) Digest;

(6) Maximum Signature Life;

(7) DNSKey Flags;

(8) DNSKey Protocol;

(9) DNSKey Algorithm;

(10) Public key;

4.8.17 **DNSSEC Delegation Signer Record Deletions.** Indicates a file type "DSDEL". This file must be sent only for incremental escrow deposits (e.g. file type "inc"); it indicates the list of domains that used to have DNSSEC delegation signer record(s) in the previous deposit that no longer have them.
The following fields shall be stored in the DSDEL file:

(1) Domain Handle; and

(2) Deletion Date.

4.8.18 **Contact information disclosure.** Indicates a file type "CONDISCL". With the exception of the Contact Handle, all the fields in this file can only be "true", "false" or empty.
The following fields shall be stored in the CONDISCL file:

(1) Contact Handle;

(2) Internationalized name;

(3) Localized name;

(4) Internationalized organization

(5) Localized organization

(6) Internationalized address;

(7) Localized address;

(8) Voice

(9) Fax

(10) Email

4.8.19 **EPP server Data Collection Policies.** Indicates a file type "DCP". These file type is related with section 2.4 of EPP, see [1]. All the fields shall only be "true", "false" or empty.
The following fields shall be stored in the DCP file:

(1) Access to All;

(2) Access to None;
(3) Access Null;
(4) Access Personal;
(5) Access Personal and other;
(6) Access Other;
(7) Statement Admin;
(8) Statement Contact;
(9) Statement Provisioning;
(10)   Statement Other;
(11)   Recipient Other;
(12)   Recipient Ours;
(13)   Recipient Public;
(14)   Recipient Same;
(15)   Recipient Unrelated;
(16)   Retention Business;
(17)   Retention Indefinite;
(18)   Retention Legal;
(19)   Retention None;
(20)   Retention Stated;
(21)   Expiry Absolute;
(22)   Expiry Relative;

4.8.20 **EPP versions supported.** Indicates a file type "EPPVERSIONS". Lists the EPP versions supported by the Registry.
The following fields shall be stored in the EPPVERSIONS file:
   (1) Version Supported;

4.8.21 **Text response languages.** Indicates a file type "LANGS". Lists the identifiers of the text response languages known by the server.
The following fields shall be stored in the LANGS file:
   (1) Language Supported; as RFCs 4646 and 4647.

4.8.22 **EPP objects supported.** Indicates a file type "EPPOBJECTS". Lists the EPP objects the server is capable of managing.
The following fields shall be stored in the EPPOBJECTS file:
   (1) Object Name;
   (2) Object URI;

4.8.23 **EPP extensions supported.** Indicates a file type "EPPEXTENSIONS". Lists the EPP extensions the Registry supports.
The following fields shall be stored in the EPPEXTENSIONS file:
   (1) Extension Name;
   (2) Extension URI;

4.9 **Extensions.** If a particular registry operator's contract requires submission of additional data, not included above, additional "extension" files shall be defined in a case by case base to represent that data which may use Domain, Contact, Name server, and Registrar Handles in order to associate that

data with these objects, and which may introduce new objects, with their own handles that may, in turn, be used to allow extension files to indicate references to these new objects. ICANN and the respective Registry shall work together to agree on such new objects' data escrow specifications.

4.10 **Compression and Encryption.** Compression shall be used to reduce transfer times between the Registry and the Escrow agent, and to reduce storage capacity requirements. Data encryption shall be used to ensure the privacy of registry escrow data.
Files processed for compression and encryption shall be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see [6]. Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC 4880, not marked as deprecated in OpenPGP IANA Registry [7], that are also royalty-free.

4.11 **Processing of data files.** The process to follow for a data file in original text format is:
(1) The file should be compressed. This specification does not require that this be done either together with or separate from the encryption process. The suggested algorithm for compression is ZIP as per RFC 4880.
(2) The compressed data shall be encrypted using the escrow agent's public key. The suggested algorithms for Public-key encryption are Elgamal and RSA as per RFC 4880. The suggested algorithms for Symmetric-key encryption are TripleDES, AES128 and CAST5 as per RFC 4880.
(3) The file may be split as necessary if, once compressed and encrypted is larger than the file size limit agreed with the escrow agent. Every part of a split file, or the whole file if split is not used, will be called a processed file in this section.
(4) A digital signature file shall be generated for every processed file using the Registry's private key. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.
(5) The processed files and digital signature files shall then be transferred to the escrow agent. This specification does not require any particular transmission mechanism though electronic delivery is preferred; acceptable options would include (but are not restricted to) electronic delivery via protocols such as SFTP or via delivery of a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices as agreed with the escrow agent.
(6) The escrow agent shall then validate every (processed) transferred data file by validating its digital signature contained in the corresponding signature file. See 7.

5. **Distribution of Public Keys.** Each of Registry Operator and Escrow Agent will distribute its public key to the other party (Registry Operator or Escrow Agent, as the case may be) via email to an email address to be specified. Each party will confirm receipt of the other party's public key with a reply email, and the distributing party will subsequently reconfirm the authenticity of the key transmitted via offline methods, like in person meeting, telephone, etc. In this way, public key transmission is authenticated to a user able to send and receive mail via a mail server operated by the distributing party. Escrow Agent, Registry and ICANN shall exchange keys by the same procedure.

6. **Notification of Deposits**. Along with the delivery of each Deposit, Registry Operator will deliver to Escrow Agent and to ICANN a written statement (which may be by authenticated e-mail) that includes a copy of the report generated upon creation of the Deposit and states that the Deposit has been inspected by Registry Operator and is complete and accurate. Escrow Agent will notify ICANN of all Deposits received, within two business days of receipt.

7.   **<u>Verification Procedure</u>**.
     {To be developed in subsequent version.}

8.   **<u>References</u>**.

[1] Extensible Provisioning Protocol (EPP), http://www.rfc-editor.org/rfc/rfc4930.txt

[2] EPP Domain Name Mapping, http://www.rfc-editor.org/rfc/rfc4931.txt

[3] EPP Host Mapping, http://www.rfc-editor.org/rfc/rfc4932.txt

[4] EPP Contact Mapping, http://www.rfc-editor.org/rfc/rfc4933.txt

[5] Common Format and MIME Type for Comma-Separated Values (CSV) Files, http://www.rfc-editor.org/rfc/rfc4180.txt

[6] OpenPGP Message Format, http://www.rfc-editor.org/rfc/rfc4880.txt

[7] OpenPGP parameters, http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml

[8] IANA Registrar IDs, http://www.iana.org/assignments/registrar-ids/

[9] IANA IDN Practices Repository, http://www.iana.org/domains/idn-tables/

[10]   Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP), http://www.rfc-editor.org/rfc/rfc4310.txt

PART B – LEGAL REQUIREMENTS

1. **Escrow Agent**. Prior to entering into an escrow agreement, the Registry Operator must contact and inform ICANN as to the identity of the Escrow Agent, and provide ICANN with contact information and a copy of the relevant escrow agreement, and all amendment thereto. ICANN must be expressly designated a third-party beneficiary of such agreement.

2. **Fees**. Registry Operator must pay, or have paid on its behalf, fees to the Escrow Agent directly. If Registry Operator fails to pay any fee by the due date(s), the Escrow Agent will give ICANN written notice of such non-payment and ICANN may pay the past-due fee(s) within ten business days after receipt of the written notice from Escrow Agent. Upon payment of the past-due fees by ICANN, ICANN shall have a claim for such amount against Registry Operator, which Registry Operator shall be required to submit to ICANN together with the next fee payment due under the Registry Agreement.

3. **Ownership**. Ownership of the Deposits during the effective term of the Registry Agreement shall remain with Registry Operator at all times. Thereafter, Registry Operator shall assign any such ownership rights (including intellectual property rights, as the case may be) in such Deposits to ICANN. In the event that during the term of the Registry Agreement any Deposit is released from escrow to ICANN, any intellectual property rights held by Registry Operator in the Deposits will automatically be licensed on a non-exclusive, perpetual, irrevocable, royalty-free, paid-up basis to ICANN or to a party designated in writing by ICANN.

4. **Integrity and Confidentiality**. Escrow Agent will be required to (i) hold and maintain the Deposits in a secure, locked, and environmentally safe facility which is accessible only to authorized representatives of Escrow Agent and (ii) protect the integrity and confidentiality of the Deposits using commercially reasonable measures. ICANN and Registry Operator will be provided the right to inspect Escrow Agent's applicable records upon reasonable prior notice and during normal business hours.

    If Escrow Agent receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposits, Escrow Agent will promptly notify the Registry Operator and ICANN unless prohibited by law. After notifying the Registry Operator and ICANN, Escrow Agent shall allow sufficient time for Registry Operator or ICANN to challenge any such order, which shall be the responsibility of Registry Operator or ICANN; provided, however, that Escrow Agent does not waive its rights to present its position with respect to any such order. Escrow Agent will cooperate with the Registry Operator or ICANN to support efforts to quash or limit any subpoena, at such party's expense. Any party requesting additional assistance shall pay Escrow Agent's standard charges or as quoted upon submission of a detailed request.

5. **Copies**. Escrow Agent may be permitted to duplicate any Deposit, in order to comply with the terms and provisions of the escrow agreement, provided that Registry Operator shall bear the expense of such duplication.

6. **Release of Deposits**. Escrow Agent will deliver to ICANN or its designee, at the Registry Operator's expense, all Deposits in Escrow Agent's possession in the event that the Escrow Agent receives a request from Registry Operator to effect such delivery to ICANN, or receives one of the following written notices by ICANN stating that:

6.1 the Registry Agreement has expired without renewal, or been terminated; or

6.2 ICANN failed, with respect to (a) any Full Deposit or (b) five Incremental Deposits within any calendar month, to receive, within five calendar days after the Deposit's scheduled delivery date, notification of receipt from Escrow Agent; (x) ICANN gave notice to Escrow Agent and Registry Operator of that failure; and (y) ICANN has not, within seven calendar days after such notice, received notice from Escrow Agent that the Deposit has been received; or

6.3 ICANN has received notification from Escrow Agent of failed verification of a Full Deposit or of failed verification of five Incremental Deposits within any calendar month and (a) ICANN gave notice to Registry Operator of that receipt; and (b) ICANN has not, within seven calendar days after such notice, received notice from Escrow Agent of verification of a remediated version of such Full Deposit or Incremental Deposit; or

6.4 Registry Operator has: (i) ceased to conduct its business in the ordinary course; or (ii) filed for bankruptcy, become insolvent or anything analogous to any of the foregoing under the laws of any jurisdiction anywhere in the world; or

6.5 a competent court, arbitral, legislative, or government agency mandates the release of the Deposits to ICANN.

6.6 Unless Escrow Agent has previously released the Registry Operator's Deposits to ICANN or its designee, Escrow Agent will deliver all Deposits to ICANN upon termination of the Registry Agreement or the Escrow Agreement.

7.   Verification of Deposits.

7.1 Within two business days after receiving each Deposit, Escrow Agent must verify the format and completeness of each Deposit and deliver to ICANN a copy of the verification report generated for each Deposit (which may be by authenticated e-mail).

7.2 If Escrow Agent discovers that any Deposit fails the verification procedures, Escrow Agent must notify, either by email, fax or phone, Registry Operator and ICANN of such nonconformity within forty-eight hours of discovery. Upon notification of such verification failure, Registry Operator must begin developing modifications, updates, corrections, and other fixes of the Deposit necessary for the Deposit to pass the verification procedures and deliver such fixes to Escrow Agent as promptly as possible. Escrow Agent must verify the accuracy or completeness of any such corrected Deposit and give ICANN notice of successful verification within twenty-four hours.

8.   Amendments. Escrow Agent and Registry Operator shall amend the terms of the Escrow Agreement to conform to this Specification 2 within ten (10) calendar days of any amendment or modification to this Specification 2. In the event of a conflict between this Specification 2 and the Escrow Agreement, this Specification 2 shall control.

[9.   Indemnity. Registry Operator shall indemnify and hold harmless Escrow Agent and each of its directors, officers, agents, employees, members, and stockholders ("Escrow Agent Indemnitees") absolutely and forever from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorneys' fees and costs, that may be asserted by a third party against any Escrow Agent Indemnitees in connection with the Escrow Agreement or the performance of Escrow Agent or any Escrow Agent Indemnitees thereunder (with the exception of any claims based on the misrepresentation, negligence, or misconduct of Escrow Agent, its directors, officers, agents, employees, contractors, members, and stockholders). Escrow Agent shall indemnify and hold harmless Registry Operator and ICANN, and each of their respective directors, officers, agents, employees, members, and stockholders ("Indemnitees") absolutely and forever from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any

other expenses whatsoever, including reasonable attorneys' fees and costs, that may be asserted by a third party against any Indemnitee in connection with the misrepresentation, negligence or misconduct of Escrow Agent, its directors, officers, agents, employees and contractors.

SPECIFICATION 3

FORMAT AND CONTENT FOR REGISTRY OPERATOR MONTHLY REPORTING

Registry Operator shall provide two monthly reports per gTLD to registry-reports@icann.org with the following content. ICANN may request in the future that the reports be delivered by other means. ICANN will use reasonable commercial efforts to preserve the confidentiality of the information reported until three months after the end of the month to which the reports relate.

1. Service Level Agreement Performance. Compare DNS, EPP and RDPS service performance for the reporting month against the SLA as described in section 4 of SPECIFICATION 6. This report shall be transmitted to ICANN electronically in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD_sla_yyyy-mm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyy-mm" is the year and month being reported. The file shall contain the following fields:

Field #	Field Name	Notes
01	epp-service-dt-min	EPP service downtime in minutes. It shall be an integer number.
02	epp-session-cmds-rtt-pct	Percentage of sampled EPP session-commands-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
03	epp-query-cmds-rtt-pct	Percentage of sampled EPP query-commands-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
04	epp-transform-cmds-rtt-pct	Percentage of sampled EPP transform-commands-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
05	rdps-dt-min	RDPS downtime in minutes. It shall be an integer number.
06	rdps-query-rtt-pct	Percentage of sampled RDPS query-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
07	rdps-update-time-pct	Percentage of sampled updates to the RDPS that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
08	dns-service-dt-min	DNS service downtime in minutes. It shall be an integer number.
09	dns-tcp-resolution-rtt-pct	Percentage of sampled TCP DNS-query-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
10	dns-udp-resolution-rtt-pct	Percentage of sampled UDP DNS-query-RTTs that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
11	dns-update-time-pct	Percentage of sampled updates to the DNS that complied with the related SLR. It shall be a real number: one or two digits with two decimals with no % sign.
12	dns-ns-dt-min-<name1>-<ip1>	Name server IP address downtime in minutes. It shall be an integer number. The name of the field shall be constructed substituting <name1> by the name of one of the name

		servers and <ip1> by one of its corresponding IP address.
13	dns-ns-dt-min-<name1>-<ip2>	" "
14	dns-ns-dt-min-<name2>-<ip1>	" "
…	…	" "

The first line shall include the field names exactly as described in the table above as a "header line" as described in section 2 of RFC 4180. Fields of the type "dns-ns-dt-min…" shall be added as needed to include all the name server's names and corresponding IP addresses. No other lines besides the ones described above shall be included.

2. Per-Registrar Activity Report. This report shall be transmitted to ICANN electronically in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD_activity_yyyy-mm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyy-mm" is the year and month being reported. The file shall contain the following fields per registrar:

Field #	Field Name	Notes
01	registrar-name	registrar's full corporate name as registered with IANA
02	iana-id	http://www.iana.org/assignments/registrar-ids
03	total-domains	total domains under sponsorship
04	total-nameservers	total name servers registered for TLD
05	net-adds-1-yr	number of domains successfully registered with an initial term of one year (and not deleted within the add grace period)
06	net-adds-2-yr	number of domains successfully registered with an initial term of two years (and not deleted within the add grace period)
07	net-adds-3-yr	number of domains successfully registered with an initial term of three years (and not deleted within the add grace period)
08	net-adds-4-yr	etc.
09	net-adds-5-yr	" "
10	net-adds-6-yr	" "
11	net-adds-7-yr	" "
12	net-adds-8-yr	" "
13	net-adds-9-yr	" "
14	net-adds-10-yr	" "
15	net-renews-1-yr	number of domains successfully renewed either

		automatically or by command with a new renewal period of one year (and not deleted within the renew grace period)
16	net-renews-2-yr	number of domains successfully renewed either automatically or by command with a new renewal period of two years (and not deleted within the renew grace period)
17	net-renews-3-yr	number of domains successfully renewed either automatically or by command with a new renewal period of three years (and not deleted within the renew grace period)
18	net-renews-4-yr	etc.
19	net-renews-5-yr	" "
20	net-renews-6-yr	" "
21	net-renews-7-yr	" "
22	net-renews-8-yr	" "
23	net-renews-9-yr	" "
24	net-renews-10-yr	" "
25	transfer-gaining-successful	transfers initiated by this registrar that were ack'd by the other registrar – either by command or automatically
26	transfer-gaining-nacked	transfers initiated by this registrar that were n'acked by the other registrar
27	transfer-losing-successful	transfers initiated by another registrar that this registrar ack'd – either by command or automatically
28	transfer-losing-nacked	transfers initiated by another registrar that this registrar n'acked
29	transfer-disputed-won	number of transfer disputes in which this registrar prevailed
30	transfer-disputed-lost	number of transfer disputes this registrar lost
31	transfer-disputed-nodecision	number of transfer disputes involving this registrar with a split or no decision
32	deleted-domains-grace	domains deleted within the add grace period
33	deleted-domains-nograce	domains deleted outside the add grace period
34	restored-domains	domain names restored from redemption period
35	restored-noreport	total number of restored names for which the registrar failed to submit a restore report
36	agp-exemption-requests	total number of AGP (add grace period) exemption requests
37	agp-exemptions-granted	total number of AGP (add grace period) exemption requests

		granted
38	agp-exempted-names	total number of names affected by granted AGP (add grace period) exemption requests

The first line shall include the field names exactly as described in the table above as a "header line" as described in section 2 of RFC 4180. The last line of each report should include totals for each column across all registrars; the first field of this line shall read "Totals" while the second field shall be left empty. No other lines besides the ones described above shall be included.

SPECIFICATION 4

SPECIFICATION FOR REGISTRATION DATA PUBLICATION SERVICES

1. **WHOIS Service.** Until ICANN specifies a different format and protocol, Registry Operator will operate a registration data publication service available via both port 43 and a website at <whois.nic.(TLD)> in accordance with RFC 3912 providing free public query-based access to at least the following elements in the following format. ICANN reserves the right to specify alternative formats and protocols, including the Internet Registry Information Service ("IRIS" – RFC 3981 and related RFCs), and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.

    1.1. **Domain Name Data:**

        1.1.1. **Query format:** whois EXAMPLE.TLD

        1.1.2. **Response format:**

        Domain Name: EXAMPLE.TLD
        Whois Server: whois.example.tld
        Referral URL: http://www.example.tld
        Updated Date: 2009-05-29T20:13:00Z
        Creation Date: 2000-10-08T00:45:00Z
        Expiration Date: 2010-10-08T00:44:59Z
        Sponsoring Registrar: EXAMPLE REGISTRAR LLC
        Sponsoring Registrar IANA ID: 5555555
        Status:DELETE PROHIBITED
        Status:RENEW PROHIBITED
        Status:TRANSFER PROHIBITED
        Status:UPDATE PROHIBITED
        Registrant ID:5372808-ERL
        Registrant Name:EXAMPLE REGISTRANT
        Registrant Organization:EXAMPLE ORGANIZATION
        Registrant Street1:123 EXAMPLE STREET
        Registrant City:ANYTOWN
        Registrant State/Province:AP
        Registrant Postal Code:A1A1A1
        Registrant Country:EX
        Registrant Phone:+1.555.555.1212
        Registrant Phone Ext: 1234
        Registrant Fax: :+1.555.555.1213
        Registrant Email:EMAIL@EXAMPLE.TLD
        Admin ID:5372809-ERL
        Admin Name:EXAMPLE REGISTRANT ADMINISTRATIVE
        Admin Organization:EXAMPLE REGISTRANT ORGANIZATION
        Admin Street1:123 EXAMPLE STREET
        Admin City:ANYTOWN
        Admin State/Province:AP
        Admin Postal Code:A1A1A1
        Admin Country:EX

Admin Phone:+1.555.555.1212
Admin Phone Ext: 1234
Admin Fax: +1.555.555.1213
Admin Email:EMAIL@EXAMPLE.TLD
Tech ID:5372811-ERL
Tech Name:EXAMPLE REGISTRAR TECHNICAL
Tech Organization:EXAMPLE REGISTRAR LLC
Tech Street1:123 EXAMPLE STREET
Tech City:ANYTOWN
Tech State/Province:AP
Tech Postal Code:A1A1A1
Tech Country:EX
Tech Phone:+1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Email:EMAIL@EXAMPLE.TLD
Name Server:NS01.EXAMPLEREGISTRAR.TLD
Name Server:NS02.EXAMPLEREGISTRAR.TLD
>>> Last update of whois database: 2009-05-29T20:15:00Z <<<

1.2. **Registrar Data:**

1.2.1. **Query format:** whois "registrar Example Registrar, Inc."

1.2.2. **Response format:**

Registrar Name: Example Registrar, Inc.
Address: 1234 Admiralty Way, Marina del Rey, CA 90292, US
Phone Number: +1.310.555.1212
Fax Number: +1.310.555.1213
Email: registrar@example.tld
Whois Server: whois.example-registrar.tld
Referral URL: www. example-registrar.tld
Admin Contact: Joe Registrar
Phone Number: +1.310.555.1213
Fax Number: +1.310.555.1213
Email: joeregistrar@example-registrar.tld
Admin Contact: Jane Registrar
Phone Number: +1.310.555.1214
Fax Number: +1.310.555.1213
Email: janeregistrar@example-registrar.tld
Technical Contact: John Geek
Phone Number: +1.310.555.1215
Fax Number: +1.310.555.1216
Email: johngeek@example-registrar.tld
>>> Last update of whois database: 2009-05-29T20:15:00Z <<<

1.3. **Nameserver Data:**

1.3.1. **Query format:** whois "NS1.EXAMPLE.TLD" or whois "nameserver (IP Address)"

1.3.2. **Response format:**

> Server Name: NS1.EXAMPLE.TLD
> IP Address: 192.65.123.56
> Registrar: Example Registrar, Inc.
> Whois Server: whois.example-registrar.tld
> Referral URL: http://www. example-registrar.tld
> >>> Last update of whois database: 2009-05-29T20:15:00Z <<<

2. **Zone File Access**

2.1. **Third-Party Access**

2.1.1 **Zone File Access Agreement.** Registry Operator will enter into an agreement with any Internet user that will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data. The terms and conditions of such agreement shall be on commercially reasonably terms as determined by Registry Operator in good faith.

Registry Operator may reject the request for access of any user that Registry Operator reasonably believes will violate the terms of specification 2.1.4 below.

2.1.2. **User Information.** Registry Operator may request each user to provide it with information sufficient to identify the user and its designated server. Such user information will include, without limitation, company name, contact name, address, telephone number, facsimile number email address and the Internet host machine name and IP address.

2.1.3. **Grant of Access.** Registry Operator will grant the User a nonexclusive, non-transferable, limited right to access Registry Operator's Server, and to transfer a copy of the top-level domain zone files, and any associated cryptographic checksum files to its Server no more than once per 24 hour period using FTP or HTTP.

2.1.4. **Use of Data by User.** Registry Operator will permit user to use the zone file for lawful purposes; provided that, (a) user takes all reasonable steps to protect against unauthorized access to and use and disclosure of the data, and (b) under no circumstances will user use the data to, (x) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or (y) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar.

2.1.5. **Term of Use.** Registry Operator will provide each user with access to the zone file for a period of not less than three (3) months.

2.1.6. **No Fee for Access.** Registry Operator will provide access to the zone file to user at no cost.

2.2 **ICANN Access.**

2.2.1. **General Access.** Registry Operator shall provide bulk access to the zone files for the registry for the TLD to ICANN or its designee on a continuous basis in the manner ICANN may reasonably specify from time to time.

[2.2.2. **Central Zone File Depository.** In the event that ICANN or its designee establishes a central zone file depository, Registry Operator will provide all zone file data to ICANN or to a third party operator of such depository designated by ICANN upon request by ICANN. Should such central zone file depository be established, ICANN may waive, at ICANN's sole discretion, compliance with Section 2.1 of this Specification 4. [**Note: This Section 2.2.2 is included for community discussion purposes as a result of prior community discussions regarding mitigation of malicious conduct. Under this provision, ICANN could take on the responsibility currently carried out by registry operators of vetting and monitoring access to zone file data by responsible parties for legitimate purposes.**]

SPECIFICATION 5

SCHEDULE OF RESERVED NAMES AT THE SECOND LEVEL IN GTLD REGISTRIES

Except to the extent that ICANN otherwise expressly authorizes in writing, the Registry Operator shall reserve names formed with the following labels from initial (i.e. other than renewal) registration within the TLD:

1.   **Example. The label "EXAMPLE**" shall be reserved at the second level and at all other levels within the TLD at which Registry Operator makes registrations.

2.   **Two-character labels**. All two-character labels shall be initially reserved. The reservation of a two-character label string shall be released to the extent that Registry Operator reaches agreement with the government and country-code manager. The Registry Operator may also propose release of these reservations based on its implementation of measures to avoid confusion with the corresponding country codes.

3.   **Tagged Domain Names.** Labels may only include hyphens in the third and fourth position if they represent valid internationalized domain names in their ASCII encoding (for example "xn--ndk061n").

4.   **Second-Level Reservations for Registry Operations.** The following names are reserved for use in connection with the operation of the registry for the TLD. Registry Operator may use them, but upon conclusion of Registry Operator's designation as of the registry for the TLD they shall be transferred as specified by ICANN: NIC, WWW, IRIS and WHOIS.

5.   **Country and Territory Names.** The country and territory names contained in the following internationally recognized lists shall be initially reserved at the second level and at all other levels within the TLD at which the Registry Operator provides for registrations:

   5.1. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time;

   5.2. the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and

   5.3. the list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

SPECIFICATION 6

REGISTRY INTEROPERABILITY, CONTINUITY, AND PERFORMANCE SPECIFICATIONS

1. **Standards Compliance**

Registry Operator shall implement and comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF) including all successor standards, modifications or additions thereto relating to (i) the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472; and (ii) provisioning and management of domain names using the Extensible Provisioning Protocol (EPP) in conformance with RFCs 3735, 3915, 5730, 5731, 5732, 5733 and 5734.

Registry Operator shall implement Domain Name System Security Extensions ("DNSSEC"). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 and 4310 and their successors, and follow the best practices described in RFC 4641 and its successors. If Registry Operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors. Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices. Registry shall also publish in its website 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.

If the Registry Operator offers Internationalized Domain Names ("IDNs"), it shall comply with RFCs 3490, 3491, and 3492 and their successors and the ICANN IDN Guidelines at <http://www.icann.org/en/topics/idn/implementation-guidelines.htm>, as they may be amended, modified, or superseded from time to time. Registry Operator shall publish and keep updated its IDN Tables and IDN Registration Rules in the IANA Repository of IDN Practices as specified in the ICANN IDN Guidelines.

Registry Operator shall be able to accept IPv6 addresses as glue records in its Registry System and publish them in the DNS. Registry Operator shall offer public IPv6 transport for, at least, two of the Registry's name servers listed in the root zone with the corresponding IPv6 addresses registered with IANA. Registry Operator should follow "DNS IPv6 Transport Operational Guidelines" as described in BCP 91. Registry Operator shall offer public IPv6 transport for its Registration Data Publication Services as defined in Specification 4 of this Agreement; e.g. Whois (RFC 3912), Web based Whois, IRIS (RFC 3981 and related RFCs). Registry Operator shall offer public IPv6 transport for its Shared Registration System (SRS) to any Registrar, no later than six months after receiving the first request in writing from a TLD accredited Registrar willing to operate the SRS over IPv6.

2. **Registry Services and Continuity**

"Registry Services" are, for purposes of the Registry Agreement, defined as the following: (a) those services that are 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 DNS servers; and dissemination of contact and other information concerning domain name server registrations in the TLD as required by this Agreement; (b) other products or services that the Registry Operator is required to provide because of the establishment of a Consensus Policy as defined in Specification 1; (c) any other products or services that only a registry operator is capable of providing, by reason of its

designation as the registry operator; and (d) material changes to any Registry Service within the scope of (a), (b) or (c) above.

Registry Operator will conduct its operations using network and geographically diverse, redundant servers (including network-level redundancy, end-node level redundancy and the implementation of a load balancing scheme) to ensure continued operation in the case of technical failure (widespread or local), business insolvency or an extraordinary occurrence or circumstance beyond the control of the Registry Operator.

Registry Operator will use commercially reasonable efforts to restore the critical functions of the registry within 24 hours after the termination of an extraordinary event beyond the control of the Registry Operator and restore full system functionality within a maximum of 48 hours following such event, depending on the type of critical function involved. Outages due to such an event will not be considered a lack of service availability.

Registry Operator shall have a contingency plan including the designation of a registry services continuity provider, and must inform ICANN of the designated provider.

In the case of an extraordinary event beyond the control of the Registry Operator where the Registry Operator cannot be contacted, Registry Operator consents that ICANN may contact the designated registry services continuity provider.

Registry Operator shall conduct registry services continuity testing at least once per year.

For domain names which are either not registered by a registrant, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFC 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

Registry Operator shall provide on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquires related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.

3. **Supported Initial and Renewal Registration Periods**

Initial registrations of registered names may be made in the registry in one (1) year increments for up to a maximum of ten (10) years.

Renewal registrations of registered names may be made in one (1) year increments for up to a maximum of ten (10) years.

4. **Performance Specifications**

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 43 min of downtime (≈ 99.9%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 99% of the queries
	UDP DNS resolution RTT	≤ 400 ms, for at least 99% of the queries
	DNS update time	≤ 15 min, for at least 99% of the updates
RDPS	RDPS availability	≤ 43 min of downtime (≈ 99.9%)
	RDPS query RTT	≤ 1500 ms, for at least 99% of the queries
	RDPS update time	≤ 15 min, for at least 99% of the updates
EPP	EPP service availability	≤ 43 min of downtime (≈ 99.9%)
	EPP session-command RTT	≤ 3000 ms, for at least 99% of the commands
	EPP query-command RTT	≤ 1500 ms, for at least 99% of the commands
	EPP transform-command RTT	≤ 3000 ms, for at least 99% of the commands

SLR. Service Level Requirement is the level of service expected for certain parameter being measured in a Server Level Agreement (SLA).

RTT. Round-Trip Time or **RTT** refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the time will be considered undefined.

IP address. Refers to IPv4 or IPv6 address without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is mentioned.

DNS. Refers to the Domain Name System as specified in RFCs 1034, 1035 and related RFCs.

DNS service availability. Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g. a TLD), to answer DNS queries from an Internet user. For the service to be considered available at some point in time, at least, two of the name servers registered in the DNS must have defined results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" over both (UDP and TCP) transports. If 51% or more of the DNS testing probes see the service as unavailable over any of the transports (UDP or TCP) during a given time, the DNS service will be considered unavailable.

DNS name server availability. Refers to the ability of a public-DNS registered "**IP address**" of a particular name server listed as authoritative for a domain name, to answer DNS queries from an Internet user. All the public DNS-registered "**IP address**" of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined results from "**DNS tests**" to a name server "**IP address**" over any of the transports (UDP or TCP) during a given time, the name server "**IP address**" will be considered unavailable.

UDP DNS resolution RTT. Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

TCP DNS resolution RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

DNS resolution RTT. Refers to either "**UDP DNS resolution RTT**" or "**TCP DNS resolution RTT**".

DNS update time. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, up until all the name servers of the parent domain name answer "**DNS queries**" with data consistent with the change made. This only applies for changes to DNS information.

DNS test. Means one non-recursive DNS query sent to a particular "**IP address**" (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. The query shall be about existing domain names. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. If the answer to a query has the TC bit set, the query will be considered unanswered. A query with a "**DNS resolution RTT**" 5-times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the "**DNS resolution RTT**" or, undefined/unanswered.

Measuring DNS parameters. Every minute, every DNS probe shall make an UDP and a TCP "**DNS test**" to each of the public-DNS registered "**IP addresses**" of the name servers of the domain named being monitored. If a "**DNS test**" gets unanswered, the tested IP will be considered as unavailable for the corresponding transport (UDP or TCP) from that probe until it is time to make a new test. The minimum number of active testing probes to consider a measurement valid is 20 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

Placement of DNS probes. Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

RDPS. Registration Data Publication Services refers to the collective of WHOIS and Web based WHOIS services as defined in "SPECIFICATION 4" of this Agreement.

RDPS availability. Refers to the ability of all the RDPS services for the TLD, to respond to queries from an Internet user with appropriate data from the Registry System. For the RDPS to be considered available at some point in time, one IPv4 and one IPv6 address for each of the RDPS services must have defined results from "**RDPS tests**". If 51% or more of the RDPS testing probes see any of the RDPS services as unavailable during a given time, the RDPS will be considered unavailable.

WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

Web-based-WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If

Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

RDPS query RTT. Refers to the collective of "**WHOIS query RTT**" and "**Web-based-WHOIS query RTT**".

RDPS update time. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, up until all the "**IP addresses**" of all the servers of all the RDPS services reflect the changes made.

RDPS test. Means one query sent to a particular "**IP address**" for one of the servers of one of the RDPS services. Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5-times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDPS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.

Measuring RDPS parameters. Every minute, every RDPS probe shall randomly select one IPv4 and one IPv6 addresses from all the public-DNS registered "**IP addresses**" of the servers for each RDPS service of the TLD being monitored and make an "**RDPS test**" to each one. If an "**RDPS test**" gets unanswered, the corresponding RDPS service over IPv4 or IPv6, as the case may be, will be considered as unavailable from that probe until it is time to make a new test. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

Placement of RDPS probes. Probes for measuring RDPS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

EPP. Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.

EPP service availability. Refers to the ability of the TLD EPP servers as a group, to respond to commands from the Registry accredited Registrars, who already have credentials to the servers. The response shall include appropriate data from the Registry System. An EPP command with " **EPP command RTT**" 5-times higher than the corresponding SLR will be considered as unanswered. For the EPP service to be considered available at during a measurement period, at least, one IPv4 and one IPv6 (if EPP is offered over IPv6) address of the set of EPP servers must have defined results from "**EPP tests**". If 51% or more of the EPP testing probes see the EPP service as unavailable during a given time, the EPP service will be considered unavailable.

EPP session-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a session command plus the reception of the EPP response for only one EPP session command. For the login command it will include packets needed for starting the TCP session. For the logout command it will include packets needed for closing the TCP session. EPP session commands are those described in section 2.9.3 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

EPP query-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a query command plus the reception of the EPP response for only one EPP query command. It does not include packets needed for the start nor close of neither the EPP nor the TCP session. EPP query

commands are those described in section 2.9.2 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

EPP transform-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a transform command plus the reception of the EPP response for only one EPP transform command. It does not include packets needed for the start nor close of neither the EPP nor the TCP session. EPP transform commands are those described in section 2.9.3 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

EPP command RTT. Refers to "**EPP session-command RTT**", "**EPP query-command RTT**" or "**EPP transform-command RTT**".

EPP test. Means one EPP command sent to a particular "**IP address**" for one of the EPP servers. Query and transform commands, with the exception of "create", shall be about existing objects in the Registry System. The response shall include appropriate data from the Registry System. The possible results to an EPP test are: a number in milliseconds corresponding to the "**EPP command RTT**" or undefined/unanswered.

Measuring EPP parameters. Every 5 minutes, every EPP probe shall randomly select one IPv4 and one IPv6 addresses from all the "**IP addresses**" of the EPP servers of the TLD being monitored and make an "**EPP tests**" to each one (IPv6 will be tested only if that transport is offered); every time it should randomly alternate between the 3 different types of commands and between the commands inside each type for testing. If an "**EPP test**" gets unanswered, the EPP service will be considered as unavailable from that probe until it is time to make a new test. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurments will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

Placement of EPP probes. Probes for measuring EPP parameters shall be placed inside or close to Registrars points of access to the Internet across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

Listing of probes. The current list of probes for DNS, RDPS and EPP can be consulted in <reference>. Registry Operator is responsible to take the necessary steps to ensure that the listed probes do not get their tests blocked by its network equipment. The list can be updated from time to time by ICANN provided it gives, at least, a 60-day notice to the Registry Operator before making the change. During that period the Registry Operator will have access to the readings for new probes, if any, without considering those measurements for SLA purposes.

Maintenance windows. Registry Operators is encouraged to do its maintenance windows for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar; any downtime, be it for maintenance or due to system failures will be noted simply as downtime and counted for SLA purposes.

SPECIFICATION 7

MINIMUM REQUIREMENTS FOR RIGHTS PROTECTION MECHANISMS

1. **Development of Rights Protection Mechanisms.** Registry Operator shall implement and adhere to any rights protection mechanisms ("RPMs") that may be mandated from time to time by ICANN. In addition to such RPMs, Registry Operator may develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party's legal rights. Registry Operator will include all ICANN mandated and independently developed RPMs in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

2. **Dispute Resolution Mechanisms.** Registry Operator will adopt and implement dispute resolution mechanisms under which third parties may challenge registration of domain names by other parties. Such dispute resolution mechanisms shall include participation in, and adherence to, the ICANN Trademark Post-Delegation Dispute Resolution Procedure (PDDRP) approved and implemented by ICANN (posted at [url to be inserted when final procedure is adopted]), as revised from time to time, including implementation of any determinations or decisions by any Post-Delegation Dispute Resolution Provider.

SPECIFICATION 8

CONTINUED OPERATIONS INSTRUMENT

1. The Continued Operations Instrument shall (a) provide for sufficient financial resources to ensure the continued operation of the basic registry functions related to the TLD set forth in Section [__] of the Applicant Guidebook posted at [url to be inserted upon finalization of Applicant Guidebook] (which is hereby incorporated by reference into this Specification 8) for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date, and (b) shall be in the form of either (i) an irrevocable standby letter of credit, or (ii) an irrevocable cash escrow deposit, each meeting the requirements set forth in Section [__] of the Applicant Guidebook posted at [url to be inserted upon finalization of Applicant Guidebook] (which is hereby incorporated by reference into this Specification 8). Registry Operator shall use its best efforts to take all actions necessary or advisable to maintain in effect the Continued Operations Instrument for a period of five (5) years from the Effective Date, and to maintain ICANN as a third party beneficiary thereof. Registry Operator shall provide to ICANN copies of all final documents relating to the Continued Operations Instrument and shall keep ICANN reasonably informed of material developments relating to the Continued Operations Instrument. Registry Operator shall not agree to, or permit, any amendment of, or waiver under, the Continued Operations Instrument or other documentation relating thereto without the prior written consent of ICANN (such consent not to be unreasonably withheld).

2. If, notwithstanding the use of best efforts by Registry Operator to satisfy its obligations under the preceding paragraph, the Continued Operations Instrument expires or is terminated by another party thereto, in whole or in part, for any reason, prior to the fifth anniversary of the Effective Date, Registry Operator shall promptly (i) notify ICANN of such expiration or termination and the reasons therefor and (ii) arrange for an alternative instrument that provides for sufficient financial resources to ensure the continued operation of the Registry Services related to the TLD for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date. Any such replacement instrument shall be on terms no less favorable to ICANN than the Continued Operations Instrument and shall otherwise be in form and substance reasonably acceptable to ICANN.

3. Notwithstanding anything to the contrary contained in this Specification 8, at any time, Registry Operator may replace the Continued Operations Instrument with an alternative instrument that (i) provides for sufficient financial resources to ensure the continued operation of the Registry Services related to the TLD for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date, and (ii) contains terms no less favorable to ICANN than the Continued Operations Instrument and is otherwise in form and substance reasonably acceptable to ICANN. In the event Registry Operation replaces the Continued Operations Instrument either pursuant to paragraph 2 or this paragraph 3, the terms of this Specification 8 shall no longer apply with respect to the Continuing Operations Instrument, but shall thereafter apply with respect to such replacement instrument(s).

REGISTRY RESTRICTIONS DISPUTE RESOLUTION PROCEDURE
(RRDRP)

INTRODUCTION

Since the early implementation stages of the New gTLD Program, implementation of a Registry Restrictions Dispute Resolution Procedure (RRDRP) has been discussed. The purpose of the RRDRP is handling complaints from a harmed organization or individual alleging that a community-based restricted gTLD registry operator was not meeting its obligations to police the registration and use of domains within the restrictions stated in the terms of the gTLD registry agreement. The need for such a procedure is based on the idea that it would not be fair to give a preference in the New gTLD Program allocation process to an applicant based on a commitment to restrict use of a TLD to a particular community, and then not require the applicant to keep its commitment." The improper acts of the registry operator might result in harm to the community or its member organizations or groups.

As stated in its 30 May 2009 Explanatory Memorandum introducing the RRDRP (http://www.icann.org/en/topics/new-gtlds/rrdrp-30may09-en.pdf), ICANN has generally avoided becoming directly involved in policing the use of domain names at the registrant level. This is appropriate in light of ICANN's mission (to coordinate the DNS "at the overall level") and in keeping with ICANN's core values (e.g., "[r]especting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination.").

Instituting a RRDRP (an independent post-delegation review process) for deciding questions of compliance with community-based domain eligibility requirements and use restrictions would have the benefit of removing ICANN from particularized decisions on Internet content and the use of domains. In the absence of an RRDRP, ICANN would be called upon to expend significant resources on gray areas of eligibility and content restrictions. Such a procedure is not intended to replace ICANN's contractual compliance responsibilities. ICANN will continue to pursue its contractual compliance activities and enforcement for all of its contracted parties, scaling up with the introduction of new top-level domains. A robust RRDRP will, however, be an additional avenue for protecting the interests of legitimate and eligible registrants within community-based restricted TLDs who otherwise could see their interests in their registrations tarnished by registrations made in violation of the promised restrictions associated with the TLD. The procedure will also provide independent judgment when it is required.

An objection complaint-based RRDRP will also be advantageous since decisions on use and eligibility will be made only when there is a real party in interest that claims to be harmed through the operation of the registry. It will limit actions to instances where a party is claiming actual harm to the community because a registry operator is not complying with restrictions in the agreement. While there may be a concern that this will create a new class of potential claimants under a theory that they are third party beneficiaries to the registry agreement between ICANN and the registry operator, that is not the intent. Indeed, the Complainant shall not be allowed to claim to be the third-party beneficiary of the registry agreement, and ICANN will ensure that its registry agreements with registry operators do not expressly or tacitly make any person a third-party beneficiary.

Registry operators will be obliged, pursuant to the registry agreement, to accept the RRDRP. ICANN would not be a party to the proceedings. The registry agreement will stipulate that ICANN and the registry operator would be bound by the Determination of the dispute resolution panel, absent extraordinary circumstances.

Initial complaints by those claiming to be harmed by the non-compliance of community restricted TLDs might be processed through an online form similar to the Whois Data Problem Report System at InterNIC.net. A nominal processing fee could serve to decrease frivolous complaints. The registry operator would receive a copy of the complaint and would be required to take reasonable steps to investigate (and remedy if warranted) the reported non-compliance. Implementation of such an online complaint process is under investigation and consideration.

The Complainant would have the option, however, to escalate the complaint if the alleged non-compliance continues. If escalated, a neutral dispute resolution panel would make the a Determination as to whether the registration complained about was inappropriate given the registration restrictions under which the registry operator agreed to operate. Below is a draft outline for how the RRDRP might be implemented.

DRAFT PROCEDURE

Parties to the Dispute

- The parties to the dispute will be the harmed organization or individual and the gTLD registry operator. ICANN shall not be a party.

Applicable Rules

- These rules for implementation of the RRDRP are intended to cover the dispute resolution proceedings generally. To the extent more than one provider is selected to implement the RRDRP, each may have additional rules and procedures that must be followed when filing a Complaint. The following are the minimal basic rules.

- Moreover, in any new gTLD registry agreement, the registry operator shall be required to agree to participate in the RRDRP and be bound by the resulting Determinations. Absent extraordinary circumstances such as bias or fraud, the Determination will be final.

Language

- The language of all submissions and proceedings under the procedure will be English.

- Parties may submit supporting evidence in their original language, provided and subject to the authority of the RRDRP expert panel to determine otherwise, that such evidence is accompanied by an English translation of all relevant text.

Communications and Time Limits

- All communications with the RRDRP provider must be filed electronically.

- For the purpose of determining the date of commencement of a time limit, a notice or other communication will be deemed to have been received on the day that it is transmitted.

- For the purpose of determining compliance with a time limit, a notice or other communication will be deemed to have been sent, made or transmitted on the day that it is dispatched.

- For the purpose of calculating a period of time under this procedure, such period will begin to run on the day following the date of receipt of a notice or other communication.

Standing

- The mandatory administrative proceeding will commence when a third-party has filed a Complaint with a RRDRP provider asserting that the complainant is a harmed organization or individual as a result of the community-based gTLD registry operator not complying with the restrictions set out in the Registry Agreement.

- Established institutions and individuals associated with defined communities are eligible to file a community objection. The "defined community" must be a community related to the gTLD string in the application that is the subject of the objection. To qualify for standing for a community claim, the objector must prove both: it is an established institution, and it has an ongoing relationship with a defined community that consists of a restricted population.

Standard

- For an claim to be successful, the claims must prove that:

  o The community invoked by the objector is a defined community;

  o There is a strong association between the community invoked and the gTLD label or string;

  o The TLD operator violated the terms of the community-based restrictions in its agreement;

  o There is a measureable harm to the Complainant and the community named by the objector.

Complaint

- **Filing:**

  The Complaint will be filed electronically. Once reviewed for technical compliance, it will be served electronically, with a hard copy and fax notice, by the RRDRP provider on the registry operator consistent with the contact information listed in the Registry Agreement.

- **Content:**

  - The name and contact information, including address, phone, and email address, of the Complainant, and, to the best of Complainant's knowledge, the name and address of the current owner of the registration.

- The name and contact information, including address, phone, and email address of any person authorized to act on behalf of Complainant..

- A statement of the nature of the dispute, which must include:

    - The particular restrictions in the Registry Agreement with which the registry operator is failing to comply; and

    - A detailed explanation of how the registry operator's failure to comply with the identified restrictions has caused harm to the complainant.

- A statement that the proceedings are not being brought for any improper purpose.

- Complaints will be limited to 5,000 words or 20 pages, whichever is less, excluding attachments.

- Any supporting documents should be filed with the Complaint.

- At the same time the Complaint is filed, the Complainant will pay a non-refundable filing fee in the amount set in accordance with the applicable RRDRP provider rules. In the event that the filing fee is not paid within 10 days of the receipt of the Complaint by the RRDRP, the Complaint will be dismissed without prejudice.

Administrative Review of the Complaint

- All Complaints will be reviewed within 10 days of submission by panelists designated by the applicable RRDRP provider to determine whether the Complainant has standing to request relief and has complied with the procedural rules.

- If the RRDRP provider finds that the Complaint complies with procedural rules, the Complaint will be deemed filed, and the proceedings will continue. If the RRDRP provider finds that the Complaint does not comply with procedural rules, the Complaint will be dismissed and the proceedings closed without prejudice to the Complainant's submission of a new Complaint that complies with procedural rules. Filing fees will not be refunded.

Response to the Objection

- The RRDRP provider will serve the complaint. The registry operator will file a response to each Complaint. The response will be filed within thirty (30) days of service the Complaint. Service will be deemed effective, and the time will start to run, upon confirmation that the written materials sent by the RRDRP provider have been received at the last known address of the registry operator.

- The Response will comply with the rules for filing of a Complaint and will contain the names and contact information for the registry operator, as well as a point by point response to the statements made in the Complaint, should be filed with the RRDRP provider and served upon the Complainant in paper and electronic form.

The filing fee must accompany the filing or the allegations in the Complaint will be sustained.

- If the registry operator fails to respond to the Complaint, it will be deemed to be in default and the allegations found in the Complaint will be deemed to have been sustained. The RRDRP provider will award an appropriate remedy in the event of default.

- Limited rights to set aside the finding of default will be established by the RRDRP provider, but in no event will they be permitted absent a showing of good cause to set aside the finding of default.

Expert

- The RRDRP provider shall select and appoint a single Expert within (30) days after receiving the response.

- Experts must be independent of the parties to the post-delegation challenge. Each RRDRP provider (if more than one is selected) will follow its adopted procedures for requiring such independence, including procedures for challenging and replacing a Expert for lack of independence.

Costs

- The RRDRP provider will determine the costs for the proceedings that it administers under this procedure in accordance with the applicable RRDRP provider Rules. Such costs will cover the administrative fees of the RRDRP provider and for the Expert.

- The RRDRP provider will estimate the costs for the proceeding and request that both the Complainant and the registry operator pay in advance the full amount of the costs. The filing fees will be credited toward the advance payment of costs. When the proceedings are terminated, the prevailing party will be refunded its advanced payment of costs.

Discovery/Evidence

- In order to achieve the goal of resolving disputes rapidly and at a reasonable cost, discovery will generally not be permitted. In exceptional cases, the Expert may require a party to provide additional evidence

- The Expert will determine whether the parties shall submit additional written statements and shall fix the short time limits for such submissions.

Hearings

- Disputes under this RRDRP will usually be resolved without a hearing.

- The Expert may decide on its own initiative, or at the request of a party, to hold a hearing. However, the presumption is that the Expert will render Determinations based on written submissions and without a hearing.

- If a request for a hearing is granted, videoconferences or teleconferences should be used if at all possible. If not possible, then the Expert will select a place for hearing if the parties cannot agree.

- Hearings should last no more than one day, except in the most exceptional circumstances.

- All dispute resolution proceedings will be conducted in English.

Burden of Proof

- The Complainant bears the burden of proving its claim, the burden should be by a preponderance of the evidence.

Remedies

- Since registrants of domain names registered in violation of the agreement restriction are not a party to the action, relief cannot take the form of deleting registrations that were made in violation of the agreement restrictions.

- The Expert will have at its disposal a variety of graduated enforcement tools including:

  - Monetary sanctions;

  - Suspension of accepting new domain name registrations in the gTLD until such time as the violation(s) is cured; or, in extraordinary circumstances,

  - Providing for the termination of a registry agreement.

- In making its Determination of the appropriate remedy, the Experts will consider the ongoing harm to the Complainant.

The Expert Determination

- The RRDRP provider and the Expert will make reasonable efforts to ensure that the Expert Determination is rendered within 45 days of the appointment of the Expert.

- The Expert will render a written Determination. The Determination will determine whether or not the Complaint is factually founded and provide the reasons for its Determination. The Determination should be publicly available and searchable on the RRDRP provider's web site.

- The Determination will state specifically when the applicable remedies are to take effect, costs and fees, however will be paid within thirty (30) days of the Expert's Determination.

Availability of Court or Other Administrative Proceedings

- The RRDRP is not intended as an exclusive procedure and does not preclude individuals from seeking remedies in courts of law.

- The parties are encouraged, but not required to participate in informal negotiations and/or mediation at any time throughout the dispute resolution process but the conduct of any such settlement negotiation is not, standing alone, a reason to suspend any deadline under the proceedings.

PROPOSED TRADEMARK POST-DELEGATION DISPUTE RESOLUTION PROCEDURE (TRADEMARK PDDRP)

INTRODUCTION

Several community participants, including the Implementation Recommendation Team (IRT) and the World Intellectual Property Organization (WIPO) have suggested that one of the rights protection mechanisms (RPM) for trademark holders should be a trademark post-delegation dispute resolution procedure (Trademark PDDRP). Various recommendations as to how such a process would be implemented have also been discussed. One point that seems to be generally accepted, is that such a procedure should only afford trademark holders the right to proceed against registry operators who have acted in bad faith, with the intent to profit from the systemic registration of infringing domain names (or systemic cybersquatting) or who have otherwise set out to use the gTLD for an improper purpose. The procedure is not intended to apply to a registry operator that simply happens to have infringing domain names within its gTLD.

Some have expressed concerns that a post-delegation procedure challenging registry operator conduct might confer third-party beneficiary rights upon non-signatories to the Registry Agreement. Further, questions have arisen as to the rights of bona fide registrants (and applicability of remedies to registrars) if they are not a party to the post-delegation dispute resolution proceedings. Such concerns are understood and can be addressed differently for alleged violations of trademark rights at the top level and for such alleged violations at the second level.

It is important to note that this Trademark PDDRP is not intended to replace ICANN's contractual compliance responsibilities. ICANN will continue to pursue its contractual compliance activities and enforcement for all of its contracted parties. This Trademark PDDRP is meant to enhance such activities and provide ICANN with independent judgment when required.

At the top level, the rights of a trademark holder to proceed against a gTLD operator for trademark infringement exist separate and apart from any contract between ICANN and a registry operator. The Trademark PDDRP simply provides a limited avenue in which to pursue rights that already exist.

Standards

Taking into account the various proposals as to the standards required to hold a registry operator liable for infringement at the top-level, it is proposed that a complainant must assert and prove:

by clear and convincing evidence that the registry operator's affirmative conduct in its operation or use of its gTLD, that is identical or confusingly similar to the complainant's mark, causes or materially contributes to the gTLD: (a) taking unfair advantage of the distinctive character or the reputation of the complainant's mark, or (b) unjustifiably impairing the distinctive character or the reputation of the complainant's mark, or (c) creating an impermissible likelihood of confusion with the complainant's mark.

An example of infringement at the top-level is where a TLD string is identical to a trademark and then, contrary to declared intentions not to infringe the rights of the mark holder, the registry operator holds itself out as the beneficiary of the mark.

Contributors mentioned above also recommend that the post-delegation procedure apply at the second level, i.e., that in some cases, the registry operator might have to answer for trademark infringing conduct in the registrations within the gTLD, rather than the TLD itself. Whether and in what manner to extend the post-delegation process to the second level must be worked through carefully. Contemplation of holding registry operators accountable for registrations in its gTLD has resulted in a number of comments regarding the standard to be applied to the registry operator, whether intervention rights should be permitted, and whether the net result of extension to the second level has a *de facto* effect of requiring registries to police all domain names and content of websites for trademark infringement. Such concerns are understood and continue to be the subject of review and discussion.

To the extent that the Trademark PDDRP is extended to the second level: some have suggested that a standard similar to that applicable to the top level apply to the second level, others have suggested that the standard be even higher to hold registry operators accountable for second level registrations in order to avoid improper results.

Accordingly, to hold a registry operator accountable for registrations at the second level, it is proposed that complainants be required to prove:

by clear and convincing evidence: (a) that there is substantial ongoing pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) of the registry operator's bad faith intent to profit from the systematic registration of domain names within the gTLD, that are identical or confusingly similar to the complainant's mark, which: (i) takes unfair advantage of the distinctive character or the reputation of the complainant's mark, or (ii) unjustifiably impairs the distinctive character or the reputation of the complainant's mark, or (iii) creates an impermissible likelihood of confusion with the complainant's mark. In this regard, it would not be nearly enough to show that the registry operator was on notice of possible of trademark infringement through registrations in the gTLD.

An example of infringement at the second level is where a registry operator repeatedly encourages registrants to register second level domain names and to take unfair advantage of the trademark to the extent and degree that bad faith is apparent.

Remedies

Regardless of whether application of the Trademark PDDRP is at the top level or at the second level, the remedies available must take into account that only the registry operator, and not the registrant or registrar, is a party to the dispute resolution proceeding. Accordingly, the applicable remedies should be limited to the registry operator and cannot provide for transfer of the infringing domain name(s) that would affect a registrant and require registrar compliance when neither are parties to the proceedings. If transfer is sought, the UDRP, or other appropriate procedure in a competent jurisdiction, can be initiated. In this regard, a balance is achieved in that the aggrieved trademark holder still has an avenue in which to bring its claims but the registry operator is only penalized for conduct in which it was an active participant.

Because intellectual property rights are at issue, there have been some suggestions that the only remedy that should be considered is cancellation of the gTLD. The IRT Final Report

envisions that the remedies would be graduated and would allow for the imposition of sanctions through forfeiture. The timing and escalation of sanctions will be specifically detailed so that this RPM produces its intended preventive effect.

Therefore, the procedure will recommend remedies that will be available for use at the discretion of the independent dispute resolution provider. These include sanctions and suspension.

In the extreme example where termination of the registry agreement is the ordered remedy, ICANN's registry continuity procedures, intended to protect registrants and provide for the ongoing resolution of domain queries, will be initiated. As there are a number of complex issues surrounding whether and to what extent the registry operator should be responsible for registrations at the second level, including the acts of registrars or registrants, it makes sense that the application of this Trademark PDDRP to the second level, and the resulting remedies, be further evaluated. With that in mind, below is a procedure for consideration and discussion.

DRAFT PROCEDURE

Parties to the Dispute

- The parties to the dispute will be the trademark holder and the gTLD registry operator. (Although there has been some suggestion that prior to commencing such a procedure, that ICANN first be notified and asked to investigate, from a practical standpoint, it does not make sense to add this layer to the procedure. It would unnecessarily slow the process.)

Applicable Rules

- This procedure is intended to cover dispute resolution proceedings generally. To the extent more than one Trademark PDDRP provider (Provider) is selected to implement the procedures, each Provider may have additional rules that must be followed when filing a Complaint. The following are general procedures to be followed by all Providers.

- In the Registry Agreement, the registry operator agrees to participate in all post-delegation procedures and be bound by the resulting Determinations.

Language

- The language of all submissions and proceedings under the procedure will be English.

- Parties may submit supporting evidence in their original language, provided and subject to the authority of the panel to determine otherwise, that such evidence is accompanied by an English translation of all relevant text.

Communications and Time Limits

- All communications with the Provider must be submitted electronically.

- For the purpose of determining the date of commencement of a time limit, a notice or other communication will be deemed to have been received on the day that it is transmitted.

- For the purpose of determining compliance with a time limit, a notice or other communication will be deemed to have been sent, made or transmitted on the day that it is dispatched.

- For the purpose of calculating a period of time under this procedure, such period will begin to run on the day following the date of receipt of a notice or other communication.

- All reference to day limits shall be considered as calendar days unless otherwise specified.

Standing

- The mandatory administrative proceeding will commence when a Complaint has been filed with a Provider asserting that the Complainant is a trademark holder (which may include either registered or unregistered marks) claiming to have been injured by the registry operator's manner of operation or use of the gTLD.

Filing of the Complaint

- The Complaint will be filed electronically. Once reviewed for technical compliance, the Provider will electronically serve the Complaint and serve a paper notice on the registry operator that is the subject of the Complaint consistent with the contact information listed in the Registry Agreement.

Content of the Complaint

- The Complaint will include:

  - The name and contact information, including address, phone, and email address, of the Complainant, and, to the best of Complainant's knowledge, the name and address of the current owner of the registration.

  - The name and contact information, including address, phone, and email address of any person authorized to act on behalf of Complainant.

  - The basis for standing; that is, why the Complainant believes it has the right to complain.

  - A statement of the nature of the dispute, which should include:

    - The particular legal rights claim being asserted, the marks that form the basis for the dispute and a short and plain statement of the basis upon which the Complaint is being filed.

    - A detailed explanation of how the Complainant's claim meets the requirements for filing a claim pursuant to that particular ground or standard.

    - A detailed explanation of the validity of the Complaint and why the Complainant is entitled to relief.

- Copies of any documents that the Complainant considers to evidence its basis for relief, including web sites and domain name registrations.

- A statement that the proceedings are not being brought for any improper purpose.

- Complaints will be limited to 5,000 words or 20 pages, whichever is less, excluding attachments.

- At the same time the Complaint is filed, the Complainant will pay a non-refundable filing fee in the amount set in accordance with the applicable Provider rules. In the event that the filing fee is not paid within 10 days of the receipt of the Complaint by the Provider, the Complaint will be dismissed without prejudice.

Administrative Review of the Complaint

- All Complaints will be reviewed by the Provider within 10 days of submission to the Provider to determine whether the Complaint contains all necessary information and complies with the procedural rules.

- If the Provider finds that the Complaint complies with procedural rules, the Complaint will be deemed filed, and the proceedings will continue. If the Provider finds that the objection does not comply with procedural rules, it will dismiss the Complaint and close the proceedings without prejudice to the Complainant's submission of a new Complaint that complies with procedural rules. Filing fees will not be refunded.

Response to the Complaint

- The registry operator will file a Response to each Complaint. The Response will be filed within twenty (20) days of service the Complaint. Service will be deemed effective, and the time will start to run, upon confirmation that the written notice sent by the Provider has been received at the last known address of the registry operator.

- The Response will comply with the rules for filing of a Complaint and will contain a point by point response to the statements made in the Complaint, should be filed with the Provider and served upon the Complainant in paper and electronic form.

- If the registry operator fails to respond to the Complaint, it will be deemed to be in default and the allegations found in the Complaint will be deemed to have been sustained. The Provider will award an appropriate remedy in the event of default.

- Limited rights to set aside the finding of default will be established by the Provider, but in no event will they be permitted absent a showing of good cause to set aside the finding of default.

- If the registry operator believes the Complaint is without merit, it will affirmatively plead in its response the specific grounds for the claim.

- The Complainant is permitted 10 days from Service to submit a reply addressing the statements made in the Response showing why the Complaint is not "without merit."

- Once the Complaint, Response and Reply (as necessary) are filed and served, a Panel will be appointed and provided with all submissions.

Panel

- Appropriately qualified panelist(s) will be selected and appointed to each proceeding by the designated Provider within thirty (30) days after receiving the response and/or reply as applicable.

- The Provider will appoint a Panel, which shall consist of one Panel member, unless all parties agree that there should be three Panelists. In the case where all Parties agree to three Panelists, selection of those Panelist will be made pursuant to the Providers rules or procedures.

- Panelists must be independent of the parties to the post-delegation challenge. Each Provider will follow its adopted procedures for requiring such independence, including procedures for challenging and replacing a panelist for lack of independence.

Costs

- The Provider will determine the costs for the proceedings that it administers under this procedure in accordance with the Provider's applicable rules. Such costs will cover the administrative fees of the Provider and for the Panel and are intended to be reasonable.

- Each party shall be required to submit the full amount of the Provider administrative fees and the Panel fees at the outset of the proceedings.

- The Provider shall refund the full amount to the prevailing party, as determined by the Panel.

Discovery

- Whether to permit discovery has been the subject of commentary. Whether and to what extent is still under review, however, given the nature of the proceeding and potential remedies, some form of written discovery might make sense, but it should be at the discretion of the Panel upon request from the Parties if the Parties cannot agree among themselves as to the scope and timing of the exchange of written discovery.

- If permitted, discovery will be limited to that for which each Party has a substantial need.

- Without a specific request from the Parties, the Provider may appoint experts to be paid for by the Parties, request live or written witness testimony, or request limited exchange of documents.

- At the close of discovery, if permitted, the Parties will make a final evidentiary submission to the Panel, the timing and sequence to be determined by the Provider in consultation with the Panel.

Hearings

- Disputes under this Procedure will be resolved without a hearing unless, in the discretion of the Panel, extraordinary circumstances require a hearing.

- The Panel may decide on its own initiative, or at the request of a Party, to hold a hearing if, extraordinary circumstances exist. However, the presumption is that the Panel will render Determinations based on written submissions and without a hearing.

- If a request for a hearing is granted, videoconferences or teleconferences should be used if at all possible. If not possible, then the Panel will select a place for hearing if the Parties cannot agree.

- Hearings should last no more than one day, except in the most extraordinary circumstances.

- All dispute resolution proceedings will be conducted in English.

Burden of Proof

- The Complainant bears the burden of proving the allegations in the Complaint, the burden should be by clear and convincing evidence.

Remedies

- The Panel will have at its disposal a variety of graduated enforcement tools such as:

  - Monetary sanctions intended to equal the financial harm to the complainant;

  - Suspension of accepting new domain name registrations in the gTLD until such time as the violation(s) is cured or a set period of time; or, in extraordinary circumstances,

  - Providing for the termination of a Registry Agreement.

- In making its Determination of the appropriate remedy, the Panel will consider the ongoing harm to the Complainant.

- While still under consideration, the Panel may also determine whether the Complaint was filed "without merit," and, if so, award the appropriate sanctions on a graduated scale, including:

  - Temporary bans from filing Complaints;

  - Imposition of costs of registry operator, including reasonable attorney fees;

- Penalty fees paid directly to DRP;

- Permanent bans from filing Complaints after being banned temporarily.

The Panel Determination

- The Provider and the Panel will make reasonable efforts to ensure that the Panel Determination is rendered within 45 days of the appointment of the Panel.

- The Panel will render a written Determination. The Determination will state whether or not the Complaint is factually founded and provide the reasons for that Determination. The Determination should be publicly available and searchable on the Provider's web site.

- The Determination will state specifically when the applicable remedies are to take effect. Any Determination as to remedy, however, will not be ordered to take effect any sooner than ten (10) business days of the Determination.

Availability of Court or Other Administrative Proceedings

- The Trademark PDDRP is not intended as an exclusive procedure and does not preclude individuals from seeking remedies in courts of law.

- In those cases where a Party provides the Provider with documented proof that a Court action was instituted prior to the filing date of the Complaint in the post-delegation dispute proceeding, the Provider may suspend or terminate the post-delegation dispute resolution proceeding.

Appeal

- All Determinations by a Panel will be immediately appealable to a court of competent jurisdiction located in either the Complainant's or the registry operator's jurisdiction.

Draft Applicant Guidebook, v3

Module 6

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.

2 October 2009

Module 6

Top-Level Domain Application –
Terms and Conditions

By submitting this application through ICANN's online interface for a generic Top Level Domain (gTLD) (this application), applicant (including all parent companies, subsidiaries, affiliates, agents, contractors, employees and any and all others acting on its behalf) agrees to the following terms and conditions (these terms and conditions) without modification. Applicant understands and agrees that these terms and conditions are binding on applicant and are a material part of this application.

1.   Applicant warrants that the statements and representations contained in the application (including any documents submitted and oral statements made and confirmed in writing in connection with the application) are true and accurate and complete in all material respects, and that ICANN may rely on those statements and representations fully in evaluating this application. Applicant acknowledges that any material misstatement or misrepresentation (or omission of material information) may cause ICANN and the evaluators to reject the application without a refund of any fees paid by Applicant. Applicant agrees to notify ICANN in writing of any change in circumstances that would render any information provided in the application false or misleading.

2.   Applicant warrants that it has the requisite organizational power and authority to make this application on behalf of applicant, and is able to make all agreements, representations, waivers, and understandings stated in these terms and conditions and to enter into the form of registry agreement as posted with these terms and conditions.

3.   Applicant acknowledges and agrees that ICANN has the right to determine not to proceed with any and all applications for new gTLDs, and that there is no assurance that any additional gTLDs will be created. The decision to review and consider an application to establish one or more gTLDs is entirely

at ICANN's discretion. ICANN reserves the right to reject any application that ICANN is prohibited from considering under applicable law or policy, in which case any fees submitted in connection with such application will be returned to the applicant.

4.   Applicant agrees to pay all fees that are associated with this application. These fees include the evaluation fee (which is to be paid in conjunction with the submission of this application), and any fees associated with the progress of the application to the extended evaluation stages of the review and consideration process with respect to the application, including any and all fees as may be required in conjunction with the dispute resolution process as set forth in the application. Applicant acknowledges that the initial fee due upon submission of the application is only to obtain consideration of an application. ICANN makes no assurances that an application will be approved or will result in the delegation of a gTLD proposed in an application. Applicant acknowledges that if it fails to pay fees within the designated time period at any stage of the application review and consideration process, applicant will forfeit any fees paid up to that point and the application will be cancelled. Except as expressly provided in this Application Guidebook, ICANN is not obligated to reimburse an applicant for or to return any fees paid to ICANN in connection with the application process.

5.   Applicant shall indemnify, defend, and hold harmless ICANN (including its affiliates, subsidiaries, directors, officers, employees, consultants, evaluators, and agents, collectively the ICANN Affiliated Parties) from and against any and all third-party claims, damages, liabilities, costs, and expenses, including legal fees and expenses, arising out of or relating to: (a) ICANN's consideration of the application, and any approval or rejection of the application; and/or (b) ICANN's reliance on information provided by applicant in the application.

6.   Applicant hereby releases ICANN and the ICANN Affiliated Parties from any and all claims by applicant that arise out of, are based upon, or are

in any way related to, any action, or failure to act, by ICANN or any ICANN Affiliated Party in connection with ICANN's review of this application, investigation or verification, any characterization or description of applicant or the information in this application, or the decision by ICANN to recommend, or not to recommend, the approval of applicant's gTLD application. APPLICANT AGREES NOT TO CHALLENGE, IN COURT OR IN ANY OTHER JUDICIAL FORA, ANY FINAL DECISION MADE BY ICANN WITH RESPECT TO THE APPLICATION, AND IRREVOCABLY WAIVES ANY RIGHT TO SUE OR PROCEED IN COURT OR ANY OTHER JUDICIAL FOR A ON THE BASIS OF ANY OTHER LEGAL CLAIM AGAINST ICANN AND ICANN AFFILIATED PARTIES WITH RESPECT TO THE APPLICATION. APPLICANT ACKNOWLEDGES AND ACCEPTS THAT APPLICANT'S NONENTITLEMENT TO PURSUE ANY RIGHTS, REMEDIES, OR LEGAL CLAIMS AGAINST ICANN OR THE ICANN AFFILIATED PARTIES IN COURT OR ANY OTHER JUDICIAL FORA WITH RESPECT TO THE APPLICATION SHALL MEAN THAT APPLICANT WILL FOREGO ANY RECOVERY OF ANY APPLICATION FEES, MONIES INVESTED IN BUSINESS INFRASTRUCTURE OR OTHER STARTUP COSTS AND ANY AND ALL PROFITS THAT APPLICANT MAY EXPECT TO REALIZE FROM THE OPERATION OF A REGISTRY FOR THE TLD.

7. Applicant hereby authorizes ICANN to publish on ICANN's website, and to disclose or publicize in any other manner, any materials submitted to, or obtained or generated by, ICANN and the ICANN Affiliated Parties in connection with the application, including evaluations, analyses and any other materials prepared in connection with the evaluation of the application; provided, however, that information will not be disclosed or published to the extent that this Applicant Guidebook expressly states that such information will be kept confidential, except as required by law or judicial process. Except for information afforded confidential treatment, applicant understands and acknowledges that ICANN does not and will not keep the remaining portion of the application or materials submitted with the application confidential.

8. Applicant certifies that it has obtained permission for the posting of any personally identifying information included in this application or materials submitted with this application. Applicant acknowledges that the information that ICANN posts may remain in the public domain in perpetuity, at ICANN's discretion.

9. Applicant gives ICANN permission to use applicant's name and/or logo in ICANN's public announcements (including informational web pages) relating to Applicant's application and any action taken by ICANN related thereto.

10. Applicant understands and agrees that it will acquire rights in connection with a gTLD only in the event that it enters into a registry agreement with ICANN, and that applicant's rights in connection with such gTLD will be limited to those expressly stated in the registry agreement. In the event ICANN agrees to recommend the approval of the application for applicant's proposed gTLD, applicant agrees to enter into the registry agreement with ICANN in the form published in connection with the application materials. Applicant may not resell, assign, or transfer any of applicant's rights or obligations in connection with the application.

11. Applicant authorizes ICANN to:

    a. Contact any person, group, or entity to request, obtain, and discuss any documentation or other information that, in ICANN's sole judgment, may be pertinent to the application;

    b. Consult with persons of ICANN's choosing regarding the information in the application or otherwise coming into ICANN's possession, provided, however, that ICANN will use reasonable efforts to ensure that such persons maintain the confidentiality of information in the application that this Applicant Guidebook expressly states will be kept confidential.

12.   For the convenience of applicants around the world, the application materials published by ICANN in the English language have been translated into certain other languages frequently used around the world. Applicant recognizes that the English language version of the application materials (of which these terms and conditions is a part) is the version that binds the parties, that such translations are non-official interpretations and may not be relied upon as accurate in all respects, and that in the event of any conflict between the translated versions of the application materials and the English language version, the English language version controls.

Glossary

Terms Applicable to this Guidebook and to the New gTLD Application Process

A-Label	The ASCII form of an IDN label. All operations defined in the DNS use A-labels exclusively.
Applicant	An entity that has applied to ICANN for a new gTLD by submitting its application form through the online application system.
Application	An application for a new gTLD lodged in connection with the terms and conditions of this guidebook. An application includes the completed Application Form, any supporting documents, and any other information that may be submitted by the applicant at ICANN's request.
Application form	The set of questions to which applicants provide responses, included in draft form as an attachment to Module 2.
Application interface	The web-based interface operated by ICANN, available at [URL to be inserted in final version of guidebook]
Application round	The complete succession of stages for processing the applications received during one application submission period for gTLDs. The terms and conditions of this guidebook are for one application round. Any subsequent application rounds will be the subject of updated guidebook information.
Application submission period	The period during which applicants may submit applications through the application interface.
Applied-for gTLD string	A gTLD string that is subject of an application.
American Standard Code for Information Interchange (ASCII)	A character encoding based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. Most modern character encodings—which support many more characters than did the

original—have a historical basis in ASCII.

Auction	A method for allocating property or goods to the highest bidder.
Auction round	Within an auction, the period of time commencing with the announcement of a start-of-round price and concluding with the announcement of an end-of-round price.
AXFR	Asynchronous full transfer, a DNS protocol mechanism through which a DNS zone can be replicated to a remote DNS server.
Bidder	An applicant who participates in an auction.
Business ID	A number such as a federal tax ID number or employer information number.
ccTLD	Two-letter top-level domains corresponding with the ISO 3166-1 country code list. See http://iana.org/domains/root/db/.
Community-based TLD	A community-based gTLD is a gTLD that is operated for the benefit of a clearly delineated community. An applicant designating its application as community-based must be prepared to substantiate its status as representative of the community it names in the application.
Community objection	An objection based on the grounds that there is substantial opposition to a gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.
Community Priority (comparative) evaluation	A process to resolve string contention, which may be elected by a community-based applicant.
Consensus policy	A policy created through the GNSO policy development process listed in Annex A of the ICANN Bylaws. See http://www.icann.org/en/general/bylaws.htm#AnnexA. A list of current consensus policies is available at http://www.icann.org/en/general/consensus-policies.htm.

Contention sets	A group of applications containing identical or similar applied-for gTLD strings.
Country-code TLD	See ccTLD.
Delegation	The process through which the root zone is edited to include a new TLD, and the management of domain name registrations under such TLD is turned over to the registry operator.
Digit	Any digit between "0" and "9" (Unicode code points U+0030 to U+0039).
Dispute Resolution Service Provider (DRSP)	An entity engaged by ICANN to adjudicate dispute resolution proceedings in response to formally filed objections.
Domain name	A name consisting of two or more (for example, john.smith.name) levels, maintained in a registry database.
Domain Name System (DNS)	The Internet Domain Name System. The DNS helps users find their way around the Internet. Every computer on the Internet has a unique address—just like a telephone number—which is a rather complicated string of numbers. Called an IP address (IP stand for Internet Protocol), the string of numbers is hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the domain name) to be used instead of the arcane IP address. So instead of typing 207.151.159.3, a user can type www.internic.net. It is a mnemonic device that makes addresses easier to remember.
Domain Name System Security Extensions (DNSSEC)	DNSSEC secures domain name lookups on the Internet by incorporating a chain of digital signatures into the DNS hierarchy.
Existing TLD	A string included on the list at http://iana.org/domains/root/db.
Extended Evaluation	The second stage of evaluation applicable for applications that do not pass the Initial Evaluation, but are eligible for further review.

G-3

Extended Evaluation period	The period that may follow the Initial Evaluation period, for eligible applications which do not pass the Initial Evaluation.
Evaluator	The individuals or organization(s) appointed by ICANN to perform review tasks within Initial Evaluation and Extended Evaluation under ICANN direction.
Evaluation fee	The fee due from each applicant to obtain consideration of its application.
Geographic Names Panel (GNP)	A panel of experts charged by ICANN with reviewing applied-for TLD strings that relate to geographical names.
Generic Names Supporting Organization (GNSO)	ICANN's policy-development body for generic TLDs and the lead in developing the policy recommendations for the introduction of new gTLDs.
Generic top-level domain	See gTLD.
gTLD	A TLD with three or more characters that does not correspond to any country code.
Hyphen	The hyphen "-" (Unicode code point U+0029).
Internet Assigned Numbers Authority (IANA)	IANA is the authority originally responsible for overseeing IP address allocation, coordinating the assignment of protocol parameters provided for in Internet technical standards, and managing the DNS, including delegating top-level domains and overseeing the root name server system. Under ICANN, IANA distributes addresses to the Regional Internet Registries, coordinate with the IETF and other technical bodies to assign protocol parameters, and oversees DNS operation.
ICANN	Internet Corporation for Assigned Names and Numbers
ICANN-accredited registrar	A company that registers domain names for Internet users. There are more than 900 ICANN-accredited registrars who provide domains to Internet users. The list of ICANN-accredited registrars is available at http://www.icann.org/en/registrars/accredited-list.html.
Internationalized Domain	A domain name including characters used in the local

G-4

Name (IDN)	representation of languages not written with the basic Latin alphabet (a - z), European-Arabic digits (0 - 9), and the hyphen (-).
Internationalizing Domain Names in Applications (IDNA)	The technical protocol used for processing domain names containing non-ASCII characters in the DNS.
IDN ccTLD Fast Track	The process for introducing a limited number of IDN ccTLDs associated with the ISO-3166 two-letter codes. See http://www.icann.org/en/topics/idn/fast-track/.
IDN table	A table listing all those characters that a particular TLD registry supports. If some of these characters are considered variants, this is indicated next to those characters. The IDN tables usually hold characters representing a specific language, or they can be characters from a specific script. Therefore the IDN table is sometimes referred to as "language variant table", "language table", "script table" or something similar.
IGO	Inter-governmental organization.
Internet Engineering Task Force (IETF)	The IETF is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Initial Evaluation period	The period during which ICANN will review an applied-for gTLD string, an applicant's technical and financial capabilities, and an applicant's proposed registry services.
International Phonetic Alphabet	A notational standard for phonetic representation in multiple languages. See http://www.langsci.ucl.ac.uk/ipa/.
IXFR	Incremental Zone Transfer, a DNS protocol mechanism through which a partial copy of a DNS zone can be replicated to a remote DNS server.
LDH (Letter Digit Hyphen)	The hostname convention defined in RFC 952, as modified by RFC 1123.
Legal Rights objection	An objection on the grounds that the applied-for gTLD string infringes existing legal rights of the objector.

Letter	Any character between "a" and "z" (in either case) (Unicode code points U+0061 to U+007A or U+0041 to U+005A).
LLC	Limited liability corporation.
Morality and public order objection	An objection made on the grounds that the applied-for gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under international principles of law.
Objection	A formal objection filed with a Dispute Resolution Service Provider in accordance with that provider's procedures.
Objection filing period	The period during which formal objections may be filed concerning a gTLD application submitted to ICANN.
Objector	One or more persons or entities that have filed a formal objection against a new gTLD application with the appropriate DRSP.
Pre-delegation test	A technical test required of applicants before delegation of the applied-for gTLD string into the root zone.
Primary contact	The person named by the applicant as the main contact for the application, and having authority to execute decisions concerning the application.
Principal place of business	The location of the head office of a business or organization.
Registrar	See ICANN-accredited registrar.
Registry	A registry is the authoritative, master database of all domain names registered in each top-level domain. The registry operator keeps the master database and also generates the zone file that allows computers to route Internet traffic to and from top-level domains anywhere in the world.
Registry Agreement	The agreement executed between ICANN and successful gTLD applicants, which appears in draft form as an attachment to Module 5.

Registry operator	The entity entering into the Registry Agreement with ICANN, responsible for setting up and maintaining the operation of the registry.
Registry services	(1) Operations of the registry critical to the following tasks: (i) the receipt of data from registrars concerning registrations of domain names and name servers; (ii) provision to registrars of status information relating to the zone servers for the TLD; (iii) dissemination of TLD zone files; (iv) operation of the registry zone servers; and (v) dissemination of contact and other information concerning domain name server registrations in the TLD as required by the registry agreement; and (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.
Registry Services Technical Evaluation Panel (RSTEP)	The Registry Services Technical Evaluation Panel is a group of experts in the design, management, and implementation of the complex systems and standards-protocols used in the Internet infrastructure and DNS. RSTEP members are selected by its chair. All RSTEP members and the chair have executed an agreement requiring that they consider the issues before the panel neutrally and according to the definitions of security and stability.
Reserved Name	A string included on the Top-Level Reserved Names List (Refer to subsection 2.1.1.2 of Module 2.)
Request for Comments (RFC)	The RFC document series is the official publication channel for Internet standards documents and other publications of the IESG, IAB, and Internet community.
Rightsholder	The person or entity that maintains a set of rights to a certain piece of property.
Root Zone	The root zone database represents the delegation details of top-level domains, including gTLDs and country-code TLDs. As manager of the DNS root zone, IANA is responsible for coordinating these delegations in accordance with its policies and procedures.

Round	See application round.
Script	A collection of symbols used for writing a language. There are three basic kinds of script. One is the alphabetic (e.g. Arabic, Cyrillic, Latin), with individual elements termed "letters". A second is ideographic (e.g. Chinese), the elements of which are "ideographs". The third is termed a syllabary (e.g. Hangul), with its individual elements represent syllables. The writing systems of most languages use only one script but there are exceptions such as for example, Japanese, which uses four different scripts, representing all three of the categories listed here.
	It is important to note that scripts which do not appear in the Unicode Code Chart are completely unavailable for inclusion in IDNs.
Second level name	A domain name that has been registered in a given top-level domain. For example, <icann.org> is a second-level name. "ICANN" is the second-level label.
Security	In relation to a proposed registry service, an effect on security by the proposed Registry Service means (1) unauthorized disclosure, alteration, insertion, or destruction of registry data, or (2) unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
Shared Registry System (SRS)	A system that allows multiple registrars to make changes to a registry simultaneously.
Stability	In relation to a proposed registry service, 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.

Standard application	An application that has not been designated by the applicant as community-based.
String	The string of characters comprising an applied-for gTLD.
String confusion objection	An objection filed on the grounds that the applied-for gTLD string is confusingly similar to an existing TLD or to another applied-for gTLD.
String Similarity Algorithm	An algorithmic tool used to identify applied-for gTLD strings that may result in string confusion.
String Similarity Panel	A panel charged with identifying applied-for gTLD strings that may result in string confusion.
String contention	The scenario in which there is more than one qualified applicant for the same gTLD or for gTLDs that are so similar that detrimental user confusion would be the probable result if more than one were to be delegated to the root zone.
TLD Application System (TAS)	The online interface for submission of applications to ICANN.
Top-level domain (TLD)	TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (right-most) dot, such as "net" in www.example.net. The TLD administrator controls what second-level names are recognized in that TLD. The administrators of the root domain or root zone control what TLDs are recognized by the DNS.
U-Label	The Unicode form of an IDN label, which a user expects to be displayed.
Unicode	Unicode is a commonly used single encoding scheme that provides a unique number for each character across a wide variety of languages and scripts. The Unicode standard contains tables that list the "code points" (unique numbers) for each local character identified. These tables continue to expand as more and more characters are digitalized. In Unicode, characters are assigned codes that uniquely

G-9

define every character in many of the scripts in the world. These "code points" are unique numbers for a character or some character aspect such as an accent mark or ligature. Unicode supports more than a million code points, which are written with a "U" followed by a plus sign and the unique number in hexadecimal notation; for example, the word "Hello" is written U+0048 U+0065 U+006C U+006C U+006F.

Uniform Domain Name Dispute Resolution Policy (UDRP)	A policy for resolving disputes arising from alleged abusive registrations of domain names (for example, cybersquatting), allowing expedited administrative proceedings that a trademark rights holder initiates by filing a complaint with an approved dispute resolution service provider.
User registration fee	The fee paid by prospective applicants for new TLDs to obtain access to the TLD Application System (TAS).
Whois	Records containing registration information about registered domain names.