Attachment 1

[IO Objection]

International Chamber of Commerce
The world business organization

International Centre for Expertise   Centre international d'expertise

NEW GENERIC TOP-LEVEL DOMAIN NAMES (“gTLD”) DISPUTE RESOLUTION PROCEDURE

OBJECTION FORM TO BE COMPLETED BY THE OBJECTOR

- *Objections to several Applications or Objections based on more than one ground must be filed separately*
- *Form must be filed in English and submitted by email to expertise@iccwbo.org*
- *The substantive part is limited to 5000 words or 20 pages, whichever is less*

***Disclaimer**: This form is the template to be used by Objectors who wish to file an Objection. Objectors must review carefully the Procedural Documents listed below. This form may not be published or used for any purpose other than the proceedings pursuant to the New GTLD Dispute Resolution Procedure from ICANN administered by the ICC International Centre for Expertise (“**Centre**”).*

References to use for the Procedural Documents

Name	**Abbreviation**
Rules for Expertise of the ICC	“**Rules**”
Appendix III to the ICC Expertise Rules, Schedule of expertise costs for proceedings under the new gTLD dispute resolution procedure	“**Appendix III**”
ICC Practice Note on the Administration of Cases	“**ICC Practice Note**”
Attachment to Module 3 - New gTLD Dispute Resolution Procedure	“**Procedure**”
Module 3 of the gTLD Applicant Guidebook	“**Guidebook**”

© International Chamber of Commerce (ICC) December 2012. All rights reserved. No part of this document may be reproduced or copied in any form or by any means, or translated, without the prior permission in writing of ICC.

Identification of the Parties, their Representatives and related entities

Objector

Name	Prof. Alain Pellet, Independent Objector
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Objector's Representative(s)

Name	Ms Héloïse Bajer-Pellet
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Daniel Müller
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Phon van den Biesen
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Sam Wordsworth
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Applicant

Name	Corn Lake, LLC
Contact	Daniel Schindler Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Other Relevant Entities

Name	-
Address	-
City, Country	-
Telephone	-
Email	-

Add separate tables for any additional relevant related entity

Disputed gTLD

gTLD Objector objects to

Name	.Charity (Application ID: 1-1384-49318)

If there is more than one gTLD you wish to object to, file separate Objections.

Objection

What is the ground for the Objection (Article 3.2.1 of the Guidebook and Article 2 of the Procedure)

□ **Limited Public Interest Objection**: the applied-for gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law.

or

☒ **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.

Check one of the two boxes as appropriate. If the Objection concerns more than one ground, file a separate Objection.

Objector’s Standing to object (Article 3.2.2 of the Guidebook and Article 8 of the Procedure)

(Statement of the Objector’s basis for standing to object, that is, why the Objector believes it meets the requirements to object.)

In accordance with Article 3.2.5 of the Guidebook, the Independent Objector (IO) is granted standing to file a formal objection, and in particular on the ground of a Community Objections “notwithstanding the regular standing requirements for such objections”. He is acting in the best interests of the public who use the global Internet and initiates and prosecutes the present objection in the public interest.

According to the same Section, the IO can object in the event that “at least one comment in opposition to the application is made in the public sphere”. This condition is met. The Application for .Charity has given rise to various comments in opposition, on the comments website of ICANN[1] and on the ICANN’s Governmental Advisory Committee (GAC) Early Warning website.[2]

Article 3.2.5 of the Guidebook states that “the IO must be and remain independent and unaffiliated with any of the gTLD applicants”. The IO has no link with the applicant under consideration and, more generally with any of the gTLD Applicants. This is equally true for his legal representatives. The IO considers himself to be impartial and independent and confirms hereby that he is acting in no other interest but the best interests of the public who use the global Internet.

[1] https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.

[2] See the Early Warning submitted by the Australian GAC member: https://gacweb.icann.org/download/attachments/22938690/Charity-AU-87032.pdf?version=1&modificationDate=1353386176000.

Description of the basis for the Objection (Article 3.3.1 of the Guidebook and Article 8 of the Procedure) - Factual and Legal Grounds

(Description of the basis for the Objection, including: a statement giving the specific ground upon which the Objection is being filed, and a detailed explanation of the validity of the Objection and why it should be upheld.)

1. The Application for .Charity has been submitted by Corn Lake, LLC.[3] The Applicant is a subsidiary of Donuts Inc., the latter being "the parent applicant for this and multiple other TLDs."[4] Donuts stated goal is "to increase competition and consumer choice at the top level."[5]

2. In the Application, it is stated that: "The TLD is a generic term and its second level names will be attractive to a variety of Internet users. Making this TLD available to a broad audience of registrants is consistent with the competition goals of the New TLD expansion program, and consistent with ICANN's objective of maximizing Internet participation. Donuts believes in an open Internet and, accordingly, we will encourage inclusiveness in the registration policies for this TLD. In order to avoid harm to legitimate registrants, Donuts will not artificially deny access, on the basis of identity alone (without legal cause), to a TLD that represents a generic form of activity and expression."[6]

3. Further, according to the Application: "The .CHARITY TLD will be of interest to the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need. This broad and diverse set includes organizations that collect and distribute funds and materials for charities, provide for individuals and groups with medical or other special needs, and raise awareness for issues and conditions that would benefit from additional resources. In addition, the term CHARITY, which connotes kindness toward others, is a means for expression for those devoted to compassion and good will. We would operate the .CHARITY TLD in the best interest of registrants who use the TLD in varied ways, and in a legitimate and secure manner."[7]

4. The Application has raised various comments in opposition. These are mainly focused on views that the string should be administered by a not for profit organization and/or that there are insufficient protection mechanisms in place such that non-*bona fide* organizations may adopt the .Charity gTLD, and create confusion in the mind of the public over what is in fact a charity.

[3] See also the public interest commitment submitted on behalf of (*inter alia*) the Applicant at: https://gtldresult.icann.org/application-result/applicationstatus/applicationchangehistory:downloadtodocument/800?t:ac=847.
[4] Application, point 18 (a).
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*

5. After an exchange of views with the Applicant, the IO has decided to file the present objection against the Application on the ground of the "community objection" as provided by Section 3.2.1 of the Guidebook.

1. Statement of the Ground upon Which the Objection is being Filed

6. According to the Guidebook, a "community objection" is warranted when "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."

7. In order to evaluate the merits of a "community objection" the Expert Panel shall "use appropriate general principles (standards)" as set out in Section 3.5 of the Guidebook, as well as "other relevant rules of international law in connection with the standards."

8. Article 3.5.4 sets out four tests which need to be met cumulatively for a "Community objection" to prevail:

- The community invoked by the objector is a clearly delineated community (Community test);
- Community opposition to the application is substantial (Substantial opposition test);
- There is a strong association between the community invoked and the applied-for gTLD string (Targeting test);
- The application creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted (Detriment test).

2. Detailed Explanation of the Validity of the Objection and Why the Objection should be Upheld

9. The four tests of a community objection provided for in the Guidebook are met in the present case. Indeed, the applied-for gTLD string .Charity targets the charity sector (a), which constitutes a clearly delineated community in the sense of the Guidebook (b). The opposition against the Application is substantial (c), and the Application creates a likelihood of material detriment to the rights and legitimate interests of the charity community (d).

a. Targeting Test

10. A “community objection” is warranted if a strong association between the community concerned and the applied-for gTLD string can be proved. In other words, the string used is or could be clearly linked to the community the rights and interests of which are at stake.

11. The Application has not been framed as a community based TLD for the benefit of the charity community. Nevertheless it targets this community, in that it explicitly targets “the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need”. This grouping, albeit very broad, must be taken to include all charitable institutions, including those that are specifically registered or regulated in some form in the states where they operate such that they must be not for profit institutions.

12. Further, as stated on the Guidebook: “All applicants should understand that a formal 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.” (Section 1.2.3.2 of the Guidebook).

13. The Guidebook also confirms that a relevant factor to be taken into account in order to evaluate the Targeting test is “[a]ssociations by the public”. The 2007 ICANN Final Report also indicates that “implicitly targeting means that the objector makes an assumption of targeting or that the objector believes there may be confusion by users over its intended use” (Implementation Guideline P). The test is therefore not limited to the assumptions and the intended use proposed in the Application, but is primarily concerned by the expectations of the average Internet users and their perception of and associations with the string. In the present case, the term “charity” is generally associated in the public mind with giving for what is seen as a good cause,[8] and likewise with not for profit institutions that are directed to some form of charitable outcome, for example (and by way of illustration only), in terms of alleviating or addressing poverty or disease, or preserving and protecting non-human species and the environment. Examples of famous charities are the Red Cross and Red Crescent organizations, CARE, Amnesty International, Oxfam, or Médecins du Monde, etc.

14. According to the Applicant’s own statements and the general use of the term by the public, there is a strong association between the charity sector and the applied for gTLD string.

[8] For a definition of “charity” as “an organization set up to provide help and raise money for those in need”, see http://oxforddictionaries.com/definition/english/charity.

b. Community Test

15. The Guidebook does not provide a clear definition of the term "community". It merely recalls that an objector "must prove that the community expressing opposition can be regarded as a clearly delineated community" (Article 3.5.4) and refers to a list of non-limited "factors" that the Expert Panel can refer to check if this test is met. It includes for example the recognition at a local/global level, the level of formal boundaries, the length of existence, the global distribution, or the size of the community.

16. The term "community" refers to a group of people living in the same place or having a particular characteristic in common.[9] The distinctive element of a community is therefore the commonality of certain characteristics. The individuals or entities composing a community can share a common territory, a common language, a common religion, a common activity or sector of activity, or other characteristics, values, interests or goals which distinguish them from others.

17. The Guidebook does not determine which kind of common characteristics, values or goals are relevant for the issue whether a given group constitutes a community, nor does it put any limits in that regard. The 2007 ICANN Final Report confirms that "community should be interpreted broadly and will include, for example, an economic sector, a cultural community, or a linguistic community."[10]

18. One of the relevant criteria is whether the group of individuals or entities can be clearly delineated from the others, and whether members of the "community [are] delineated from Internet users in general"[11] with reference to their common characteristics. The recognition of the community among its members, on the one hand, and by the general public at a global or a local level, on the other hand, depending on its actual distribution, is in that regard a useful factor to be taken into account.

19. In the present case, as noted above, the community targeted by the Applicant is composed of "the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need". Although this is a broader group than charities *per se*, it clearly includes charities and charitable organizations.

20. Charities and charitable organizations exist everywhere in the world. They are generally characterized by their charitable aims, and often by the status of a not for profit institution. Further, as noted in the GAC Early Warning made by Australia: "In many

[9] See http://oxforddictionaries.com/definition/english/community.
[10] Implementation Guideline P, http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm
[11] Evaluation question No 20 of the Guidebook, Attachment to Module 2.

jurisdictions, charitable organizations are exempted from a range of regulatory requirements that apply to for-profit entities, and are funded through donations or public money."[12] In the light of their particularities, their common goals, interests and values, charities are to be delineated from Internet users in general, and are rightly seen as constituting a community. In addition, public comments made on the community ground point to the existence of such a community, being the charity community or the community of charitable organizations, and generally express an opinion in the name of the designated community.

21. While the Applicant is understood to take issue with the IO's view that the "interested community is not institutionalised and straddles the border between different stakeholders of the community of charitable organisations", that in no sense means that there is no community consistent with the Guidebook. An organized community – i.e., a community that has some entity dedicated to the community and its activities – has usually clearer formal boundaries described in terms of membership or registration. The situation is different in case of communities that are less structured or organized, like those based on a common place of origin or a common language or a common activity or common set of goals or interests or values. This is the case of the charity community, which is nonetheless a clearly recognizable community, distinct from others, at a local, national, and also global level. Organization and structure, even if they can help to identify a community and its delineation, are not relevant distinctive criteria for the existence of a clearly delineated community or a sign of lack of cohesiveness.

c. *Substantial Opposition Test*

22. According to the Guidebook, a "Community objection" is warranted in the event of "substantial opposition within the community". This test and its scope of application depend largely on the circumstances and of the context of each case.

23. The Guidebook includes several factors, which the Expert Panel can use in order to determine if such "substantial opposition" with regard to an application exists. These factors include the number of expressions of opposition relative to the composition of the community, the representative nature of entities expressing opposition, the level of recognized stature or weight among sources of opposition, distribution or diversity among sources of expressions of opposition, historical defense of the community in other contexts, and costs incurred by the objector in expressing opposition, including other channels the objector may have used to convey opposition.

[12] https://gacweb.icann.org/download/attachments/22938690/Charity-AU-87032.pdf?version=1&modificationDate=1353386176000.

24. This list is not limitative. It focuses on the number of oppositions expressed or the representative nature of those having expressed opposition, i.e., the part of the community represented by those having expressed opposition and its significance with regard to the community in its entirety. These criteria are useful, in particular in the case of well-organized and structured communities. They are more difficult to apply in case of communities which lack organizational structures or clear representation.

25. A mere numerical criterion was certainly not the intent of the authors of the Guidebook and the Expert Panel is not limited to a mere numerical analysis balancing the number of those having expressed opposition or are deemed to be represented by those having expressed opposition, on the one hand, and the overall size of the concerned community, on the other hand. The word “substantial” cannot be defined as limited in that way. If it can certainly refer to an important size or number, it is also used for something of “considerable importance” or “considerable … worth”.[13] Not only the number of opposition should be taken into account, but also the material content of comments and oppositions expressed by those concerned, and in particular, the importance of the rights and interests at stake.

26. The fact that the IO was granted the possibility to file “Community Objections” confirms the necessary broad meaning of the terms “substantial opposition”. Indeed, the IO would not file a formal “Community objection” if a single established institution is better placed to represent the community concerned[14]. His role is to defend the public interests and to act on behalf of the public for the defense of rights and interests of communities which lack institutions which obviously could represent the community in the present context..

27. In the present case, a number of comments in opposition have been posted on the public comments website,[15] including by the Charity Commission for England and Wales, which “is a government department established as the independent registrar and regulator of charities in England and Wales”, the National Council for Voluntary Organisations, which brings together “just under 10,000 organizations” in the United Kingdom, and the Association of Charitable Foundations, which “is the umbrella body and membership organisation for grant-making charitable trusts and foundations in the United Kingdom, representing over 330 members”.[16]

[13] See http://oxforddictionaries.com/definition/english/substantial.

[14] See i.e., http://www.independent-objector-newgtlds.org/english-version/the-independent-objector-s-comments-on-controversial-applications/africa-general-comment/.

[15] https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.

[16] See the details given by each participant at https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.

28. Thus, a significant portion of the involved community, mainly (but not exclusively) from the United Kingdom, have expressed concerns to the launch of a new gTLD related to the charity sector. It is noted that those responding include important regulatory and representative bodies from the United Kingdom.

29. The reasons for the opposition expressed on the public comments website are similar in nature. While various participants have expressed the view that the string .Charity should be a community based gTLD / run by a not for profit organization, the common underlying concern is based on potential harm to the system of trust on which charities and charitable giving are largely dependent. In this respect, the following view expressed by the Charity Commission for England and Wales was typical:

> "As a charity regulator we believe it is crucial that the '.charity' gTLD is administered by an organisation that fully understands the risks involved in its inappropriate use and actively considers applications with those risks in mind. They should not, for example, simply look to maximise its use for purely commercial reasons where this might damage public trust and confidence in charities. In allowing organisations to use this gTLD they may also need to consider the impact of legal restrictions on organisations falsely representing themselves as charities.
>
> Charities in England and Wales - and, we assume, elsewhere - depend on public confidence for funding and other forms of support such as volunteering. Maintaining this confidence is crucial if charities are to be successful. If, however, the gTLD is administered with no regard for this we are concerned that could lead to confusion, misunderstanding and, perhaps, deliberate abuse that will undermine that confidence That could significantly damage charities if public support drops as a result. It may also of course have an adverse impact on the value of the .charity gTLD."

30. To similar effect, the Office of the Scottish Charitable Regulator stated (albeit as part of a legal rights objection):

> "Charities depend on public trust to raise funds from the public and other bodies and to generate support from volunteers and the communities in which they operate. Exploiting the term 'charity' in an unregulated manner for commercial gain would be detrimental to all charities.
>
> Therefore, we would expect that any proposal for a '.charity' gTLD to include strict eligibility criteria for applicants and require evidence from applicants of the award of charitable status by the appropriate regulatory body."

31. In addition, the Australian member of the GAC has expressed concern in an Early Warning that raises similar issues, stating that "Charity" is "linked to a regulated market sector" and that applicants do not "appear to have proposed sufficient mechanisms to minimize potential consumer harm". He underlined that "in many jurisdictions, charitable organizations are exempted from a range of regulatory requirements that apply to for-profit entities, and are funded through donations or public money" and that "without additional

protections, this proposed TLD could result in misuse and consumer harm, and could result in damage to the trust that consumers and governments place in legitimate charities".[17]

32. Such an Early Warning is an indication that "the application is seen as potentially sensitive or problematic by one or more governments" and of the substantial opposition it generates (Article 1.1.2.4 of the Guidebook).

33. Even if the opposition has largely emanated from the UK and Australian jurisdictions, concerns voiced are without doubt substantial and of much more general application. In these circumstances, the opposition against the Application must be considered as being substantial.

d. Detriment Test

34. A community objection is warranted if the Application creates "a likelihood of detriment to the rights or legitimate interests of the community or to users more widely".[18] This test is met in the present case.

35. The Guidebook includes some guidance with regard to the Detriment test, which needs to be addressed with regard to the specific elements and particularities of each application, on the one hand, and the interests and rights of the community to which the applied-for gTLD can be targeted, on the other hand. The material detriment can result from harm to reputation of the community, interference with the community's core activities, economic or other concrete damage to the community or significant portions of the community. In order to assess the likelihood of such harm or damage, the Expert panel can take into account a variety of factors, including the dependence of the community on the DNS for its core activities, the intended use of the gTLD as evidenced in the Application, but also the importance of the rights and interests exposed for the community targeted and for the public more generally.

36. The Guidebook puts particular attention to the issue whether 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 and community interests. In such a case, it is more than likely that the rights and interests of the community will be detrimentally affected by operation of the gTLD as projected by the applicant.

[17] See https://gacweb.icann.org/download/attachments/22938690/Charity-AU-49318.pdf?version=1&modificationDate=1353386080000.

[18] Implementation Guideline P, http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm.

37. The charity sector is strictly regulated in certain jurisdictions (at least), as is consistent with the need for the public to retain the trust that money donated or services volunteered to charities will be directed towards the charitable purposes that given donors have had in mind. To this end, specific regulations and safeguards may serve to protect both individual members of the public and the public interest in such trust being retained. That public interest includes the interests of the charities themselves, whose existence and operations would be threatened by a loss of public trust. It ultimately also includes the interests of those benefitting from charitable organizations, such as those in poverty or at risk of human rights violations.

38. It follows that the reputation of charities amongst (in particular) donors and potential donors is of the utmost importance. The high reputation of the charity community is key to the attraction of gifts of money and time and services generally to this community, and thus for maintaining and developing the very broad range of charitable activities that exist today. This point has been made in various different ways in the comments that have been posted on the public comments website.[19] Examples of this have already been given under (c) above. To take a further example in the form of the views of one locally focused UK charity (Voluntary Action Leeds): “The charity 'brand' largely operates on the basis of trust: that is, people give their time and money to charities of their own free will. In the United Kingdom charities are regulated by the Charity Commission and HMRC, giving the public confidence and trust that charities are running for public benefit. In Leeds we see the benefits of this trust in charities every day: the huge contribution of volunteers to our local economy, philanthropic giving and engagement in the life of the city.”[20]

39. The potential for harm if the gTLD were administered without mechanisms for protecting public trust in charities is identified e.g. by the view of the Charity Commission for England and Wales, where it points to the scope for confusion, misunderstanding and, perhaps, deliberate abuse, resulting in turn in significant damage to charities if public support dropped as a result. As to such deliberate abuse, one participant (Goodwill Industries International Inc) stated that it was “particularly concerned that new TLDs for charitable terms will increase the opportunity for fraudsters and cybersquatters to trade off the good will and trust of well-known non-profit names and charitable terms like the applied-for string by confusing Internet users with domain names made up of those names and terms and soliciting money and/or phishing for private information for their own benefit. These activities, which already cost charities billions of dollars each year, not only divert funds from non-profits, they erode the trust upon which these organizations rely. Allowing this to occur would

[19] https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.
[20] See at https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments.

cause a material detriment to the community which the string obviously targets, as well as to society at large." [21]

40. Notwithstanding certain of the comments received, the IO has not formed the view that this string need necessarily be operated by a non-profit organization, provided that the applicant for the gTLD offers adequate guarantees that the values specific to the charities sector will be respected.

41. The Applicant, however, has not addressed the specific needs of the charity community in its proposed management of the gTLD .Charity, and there are three key factors that demonstrate the likelihood of detriment to the charity community.

42. First, even though the Applicant has recognized "the level of end-user trust potentially associated with this string"[22] and has proposed some additional protection mechanisms[23] – like it has done for other Applications submitted by Donuts subsidiaries[24] – it is striking that the Application has not been framed by Donuts and its subsidiary as a community based gTLD. In so doing the Applicant avoids certain consequences in terms of the evaluation of the Application and the terms under which it will be operated. In particular, the Applicant will not be committed to establish requirements for registration by members of the TLD community and use of registered domain names in conformity with the stated purpose of the community-based TLD.[25] The Applicant does not recognize the existence of a delineated charity community, and has made no commitment to operate the .Charity gTLD for the benefit and in the interest of the charity community, taking into account the public interest goals associated with this community.

43. Secondly, the Application does not propose any eligibility criteria for the string. In the Application – as well in other Applications made by other affiliates of Donuts – it is explained:

> "We recognize some applicants seek to address harms by constraining access to the registration of second level names. However, we believe attempts to limit abuse by

[21] The Applicant does recognize the scope for abuse: see Application, point 18(a). For example, it is said there that "access to the countless benefits and opportunities which the internet offers can often be hindered when navigating the ever-expanding sea of irrelevant and sometimes malicious content which also exists, and this is as true of online charitable services as anything else."

[22] Application, point 18 (a).

[23] These four additional protection mechanisms are the followings:

"1. For this string, to supplement the periodic audit documented above, a deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes.

2. Exclusion of registrars with a history of poor compliance;

3. Regular monitoring by the registry of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes; and

4. In addition to registry-based procedures, requirements that registrars have a 24/7/365 abuse contact, and remediation and takedown processes." (*Ibid.*)

[24] See, e.g., the Application for .Creditcard (Application ID 1-1412-63109).

[25] Article 2.18, Draft New gTLD Registry Agreement (annexed to the Guidebook).

> limiting registrant eligibility is unnecessarily restrictive and harms users by denying access to many legitimate registrants. Restrictions on second level domain eligibility would prevent law-abiding individuals and organizations from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD. As detailed throughout this application, we have struck the correct balance between consumer and business safety, and open access to second level names."[26]

44. Donut's preference is to address abuse if it occurs, rather than (as it would see it) to needlessly over-regulate usage and diminish a gTLD's consumer value before it becomes available. Without prejudging whether this approach to management and operation is suitable and appropriate for other gTLDs, safety and security measures which are only directed at remedying problems and abuses if and when they occur do not meet the specific needs and requirements of the charity community, of users and the public interest. The absence of preventive security measures assuring the integrity and the trustworthy nature of the entities represented and the information provided under the gTLD .Charity, e.g., through stringent eligibility criteria established in collaboration with the community and its stakeholders, is likely to have detrimental effects on trust in the community and the TLD.

45. Thirdly, the security mechanisms proposed by the Applicant's parent company and aimed at reacting to abuse are unlikely to meet the specific requirements and needs of the charity community. The Applicant has made no commitment concerning the specific content of the "Anti-Abuse Policy" described in point 28 of its Application, nor has it given any information concerning the elaboration of this policy. It is not suggested that the charity community, which is targeted by the TLD string, or any of its stakeholders will be associated in the elaboration of this policy or its implementation. To the contrary, the Applicant has expressly reserved the right to react to abuse and to take the appropriate steps "at its sole discretion and at any time and without limitation".[27] In addition, the proposed "Anti-Abuse Policy" has not been specifically elaborated in order to meet the needs of the charity community, taking into account the importance of users' protection and confidence. To the contrary, the proposed policy appears to be largely identical to the policy proposed by other Donuts' subsidiaries in relation to strings with different features (see e.g. in relation to the Application submitted by Binky Frostbite, LLC, a subsidiary of Donuts, for the gTLD .Creditcard[28]).

46. The absence of preventive security measures assuring the charitable nature, the integrity and also the trustworthiness of the entities represented and the information provided under the gTLD .Charity, e.g., through stringent eligibility criteria established in advance in

[26] Application, point 18 (a).
[27] Application, point 28 (3.0).
[28] Application ID 1-1412-63109.

collaboration with the community and its stakeholders, creates a likelihood of detriment to the rights or legitimate interests of the charity community, to users and to the general public.

Remedies Requested

(Indicate the remedies requested.)

The Independent Objector requests the Expert panel to hold that the present objection is valid. Therefore, the Expert panel should uphold the present Objection against this .Charity Application.

In addition, the Independent Objector requests that its advance payments of costs shall be refunded in accordance with Article 14 (e) of the Procedure (Attachment to Module 3 - New gTLD Dispute Resolution Procedure).

Communication (Article 6(a) of the Procedure and Article 1 of the ICC Practice Note)

A copy of this Objection is/~~was~~ transmitted to the Applicant on 13 March 2013 by e-mail to the following address Contact Information Redacted

A copy of this Objection is/~~was~~ transmitted to ICANN on 13 March 2013 by e-mail to the following address: newgtld@icann.org

Filing Fee (Article 1 Appendix III to the Rules and Article 8(c) of the Procedure)

In accordance with Article 3.2.5 of the Guidebook, ICANN is responsible to provide the funding on behalf of the Independent Objector.

The Independent Objector hereby explicitly grants ICC the right to contact ICANN directly with regard to any payment matters for the Objections.

Description of the Annexes filed with the Objection (Article 8(b) of the Procedure)

List and Provide description of any annex filed.

-

Date: 12 March 2013

Signature: ___

Attachment 2

[Corn Lake Opposition]

International Centre for Expertise   Centre international d'expertise

NEW GENERIC TOP-LEVEL DOMAIN NAMES ("gTLD")
DISPUTE RESOLUTION PROCEDURE

RESPONSE FORM TO BE COMPLETED BY THE APPLICANT

- *Applicant responding to several Objections or Objections based on separate grounds must file separate Responses*
- *Response Form must be filed in English and submitted by email to expertise@iccwbo.org*
- *The substantive part is limited to 5000 words or 20 pages, whichever is less*

***Disclaimer**: This form is the template to be used by Applicants who wish to file a Response. Applicants must review carefully the Procedural Documents listed below. This form may not be published or used for any purpose other than the proceedings pursuant to the New GTLD Dispute Resolution Procedure from ICANN administered by the ICC International Centre for Expertise ("**Centre**").*

References to use for the Procedural Documents

Name	**Abbreviation**
Rules for Expertise of the ICC	"**Rules**"
Appendix III to the ICC Expertise Rules, Schedule of expertise costs for proceedings under the new gTLD dispute resolution procedure	"**Appendix III**"
ICC Practice Note on the Administration of Cases	"**ICC Practice Note**"
Attachment to Module 3 - New gTLD Dispute Resolution Procedure	"**Procedure**"
Module 3 of the gTLD Applicant Guidebook	"**Guidebook**"

Annex A defines capitalized terms and abbreviations in addition to or in lieu of the foregoing.

ICC International Centre for ADR   Centre international d'ADR de la CCI
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 30 52 Fax +33 (0)1 49 53 30 49
E-mail expertise@iccwbo.org Website www.iccexpertise.org

© International Chamber of Commerce (ICC) D 2012. All rights reserved. No part of this document may be reproduced or copied in any form or by any means, or translated, without the prior permission in writing of ICC.

Identification of the Parties and their Representatives

Applicant

Name	Corn Lake, LLC
Contact person	Daniel Schindler
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Objector

Name	Prof. Alain Pellet, Independent Objector
Contact person	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Copy the information provided by the Objector.

Applicant's Representative(s)

Name	The IP & Technology Legal Group, P.C. dba New gTLD Disputes http://www.newgtlddisputes.com
Contact person	John M. Genga, Don C. Moody
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Add separate tables for any additional representative (for example external counsel or in-house counsel).

Applicant's Contact Address

Name	The IP & Technology Legal Group, P.C. dba New gTLD Disputes http://www.newgtlddisputes.com
Contact person	John M. Genga, Don C. Moody
Address	Contact Information Redacted
City, Country	
Telephone	
Email	Contact Information Redacted Copies to: Contact Information Redacted , ATTN: Daniel Schindler Contact Informat on Redacted ATTN: Jon Nevett

This address shall be used for all communication and notifications in the present proceedings. Accordingly, notification to this address shall be deemed as notification to the Applicant. The Contact Address can be the Applicant's address, the Applicant's Representative's address or any other address used for correspondence in these proceedings.

Other Related Entities – Objector's Representatives

Name	Ms Héloïse Bajer-Pellet
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	Mr. Daniel Müller
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	Mr. Phon van den Biesen
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	Mr. Sam Wordsworth
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Disputed gTLD

gTLD Applicant has applied for and Objector objects to:

Name	<.CHARITY> – Application ID 1-1384-49318, ICC EXP/395/ICANN/12

Objection

The Objector filed its Objection on the following Ground (Article 3.2.1 of the Guidebook and Article 2 of the Procedure)

□ **Limited Public Interest Objection**: the applied-for gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law.

or

☒ **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.

Copy the information provided by the Objector.

Point-by-Point Response to the claims made by the Objector (Article 3.3.3 of the Guidebook and Article 11 of the Procedure)

(Provide an answer for each point raised by the Objector.)

A.

INTRODUCTION

1. Applicant Proposes a <.CHARITY> gTLD to Carry Out ICANN's Objectives.

As described below, the Independent Objector (hereinafter "Objector") lacks standing to make this objection and, even if he had standing, the Objection would easily fail on the merits. First however, it is important to note that ICANN adopted its new gTLD program to enhance choice, competition and expression in the namespace. AGB Preamble, § 1.1.2.3, and Mod. 2 Attmt. at A-1. Such generic TLDs bring competition to registries, which have not experienced it in a world that has known little more than <.COM>, as well as the opportunity for more consumers to enjoy the benefits of such competition.

To accomplish ICANN's goals, Donuts has applied for <.CHARITY> among 307 gTLDs, to offer domains on subjects that otherwise may not have their own forums. Nevett Dec. ¶¶ 4-6 (**Annex B**). This gTLD represents one of a number of niche offerings by Donuts in an expanding Internet "shopping mall." It gives users the choice of a specialty experience as an alternative to the sprawling "department store" environment of incumbent registries such as <.COM>. *Id.* ¶¶ 6, 8.

The instant Objection would thwart these important benefits. It urges that a <.CHARITY> TLD should operate with strict registration policies such that only charitable organizations, and no one else, could access it. This would close an entire segment of the Internet to the many potential uses of a common word's multiple meanings. It also ignores the unprecedented levels of security that Donuts would bring to the TLD.

Contrary to what Objector himself might prefer, and consistent with what ICANN seeks, Applicant would make the <.CHARITY> registry open to all consumers. This would create paths of communication more expansive than the narrow use to which Objector believes the TLD should be put. Applicant can and will do this with greater protections than the namespace has ever known. A for-profit business, for example, might choose to describe its charitable giving practices on a .charity website (e.g. <Verizon.charity>, <USBC.charity>). Individuals might like to use it to blog about a project. Donuts does not believe that people and entities should be restricted from a <.CHARITY> registry just because the Objector thinks that it should be limited to certain groups. Such a restriction violates the fundamental rights of freedom of expression and has no place in the Internet or the New TLD program.

Donuts is a well prepared, amply resourced and highly qualified group committed to offering consumers new and varied generic domain name alternatives through safe, stable and secure registry operations. Its team consists of industry veterans with long histories of contributing to ICANN's policymaking process, successfully launching gTLDs, building industry-leading companies, and bringing innovation, value and choice to the domain name marketplace. Nevett Dec. ¶¶ 3 (**Annex B**).

Since the inception of the new gTLD program, Donuts executives have participated actively in its multi-stakeholder process of developing the Guidebook and other elements of the program. As a direct result of Donuts' involvement, ICANN requires new gTLD operators to implement more than a dozen safeguards that it never did and still does not require of current gTLD registries. Donuts will run the <.CHARITY> gTLD not only with those mechanisms, but with a dozen more that go well beyond what ICANN requires. *Id.* ¶¶ 9-12. As such, the gTLD will operate much more safely than any currently does, while maintaining an open environment consistent with ICANN's objectives in expanding the namespace.

2. *Objector fails to meet his burden to prove the four requisite elements for this community objection.*

In the instant case, Objector does not satisfy his burden of demonstrating any of the requisite elements delineated by ICANN to support his community objection to the <.CHARITY> application and cannot do so for an everyday word that Applicant offers for generic Internet use not targeted at a community. Specifically, ICANN has made clear:

> There is a presumption generally in favor of granting new gTLDs to applicants who can satisfy the requirements for obtaining a gTLD – and, hence, a corresponding burden upon a party that objects to the gTLD to show why that gTLD should not be granted to the applicant.

http://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf.

Objector does not speak for a clearly delineated community that can properly bar from the Internet a word in the common lexicon. Nor does Objector show that the claimed "community" has substantial opposition to, or a strong association with, Applicant's proposed string.

Finally, most significantly, Objector demonstrates no material detriment to the purported community. Objector's supposition of improper activity does not constitute proof that it will occur. Moreover, Applicant has established protective mechanisms that exceed ICANN's requirements. Those procedures – not this Objection – provide the proper means to address issues that have not yet arisen. In fact, the Applicant proposes to operate the TLD in a fashion extremely beneficial to those interested in charity and related issues.

Applicant has the same free speech rights as the general public to conduct its affairs using ordinary words from the English language. To hold otherwise would negate such rights, impede the growth of and competition on the Internet, and set dangerous precedent that takes choice away from the many and places control in the hands of a few.

B.

EVEN AS AN INDEPENDENT OBJECTOR, STANDING IS LACKING WHERE, AS HERE, NO CLEARLY DELINEATED COMMUNITY EXISTS

ICANN has authorized an Independent Objector to file community objections only "against 'highly objectionable' gTLD applications to which no objection has been filed." AGB § 3.2.5 at 3-10. While the Guidebook grants him standing to file community objections "notwithstanding the regular standing requirements for such objections," *id.*, he nevertheless still must act on behalf of a "clearly delineated community." AGB § 3.2.2.4. "The community named by the objector must be … strongly associated with the applied-for gTLD string." *Id.* at 3-7. In other words, the word "charity" must readily bring to mind some "community" recognized by that designation. Merely stating that proposition reveals its folly.

Clear delineation of a charity "community" hardly seems possible. The word "charity" describes a subject, not a community, which interests and affects numerous and diverse individuals and organizations not susceptible of neat classification. Arguably – indeed, highly plausibly – the entire world population has a fundamental interest in, and is impacted by, charity or the benevolent goodwill toward humanity.

The notion of a charity "community," which would allow a single party such as Objector to prevent the use of a dictionary term to the exclusion of all others, defies reason. Such a scheme contravenes the open nature of the Internet and the intent of ICANN in adopting the new gTLD program. *See* Nevett Dec. ¶ 4 (**Annex B**). As such, this lack of an actual community is unsurprisingly why no actual objections were filed against this TLD by anyone in the actual purported community that the Objector is trying to represent.

Even though the Guidebook makes an initial grant of standing to the Objector, he must object on behalf of a clearly defined community to maintain that standing. The Panel should dismiss the Objection on standing alone. It need never consider the substance of the Objection. Nevertheless, we reveal its absence of merit below.

C.

THE OBJECTION SHOULD BE REJECTED

A valid community objection requires "substantial opposition from a significant portion of the community to which the string may be targeted." AGB § 3.5.4. This gives Objector the burden of proving: (1) existence of a clearly delineated community; (2) substantial opposition to the application by the community; (3) a strong association between that community and the subject string; **and** (4) a "likelihood" that the Application will cause "material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be … targeted." *Id.* at 3-22. "The objector must meet all four tests … for the objection to prevail;" failure on any *one* compels denial. *Id.* at 3-25. Objector here meets none.

1. Objector Invokes No Clearly Delineated Community.

Applicant has already shown above that Objector does not represent a "clearly delineated" community. However, Objector necessarily must overcome a more stringent test on the merits than he need do for standing. ICANN would have no reason to make "clearly delineated" a substantive element of the objection if it meant nothing more than the criterion for standing. Rules "should be interpreted so as not to render one part inoperative." *Colautti v. Franklin*, 439 U.S. 379, 392 (1979). *See also United States v. Menasche*, 348 U.S. 528, 538-39 (1955).

To meet the substantive test of clearly delineated community, an objector must prove this by providing the Panel evidence of the following: (1) the level of public recognition of the group as a community at a local and/or global level; (2) the level of formal boundaries around the community and what persons or entities are considered to form the community; (3) the length of time the community has been in existence; (4) the global distribution of the community; and (5) the number of people or entities that make up the community. AGB § 3.5.4 at 3-22, 3-23.

Objector fails to provide any evidence of a clearly delineated "charity community." This plain fact is showcased by his own definition of the community at issue: "millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need." Objn at 9, ¶ 19. He elaborates that "[a]lthough this is a broader group than charities *per se*, it clearly includes charities and charitable organizations." *Id.*

There are at least three pivotal problems with the purported community articulated and represented by Objector. First, while the broader group of "millions of persons and organizations worldwide involved in philanthropy…" can clearly be characterized as global (one of the factors relied upon by ICANN) it has *no boundaries whatsoever* – formal or otherwise. This so-called community conceivably consists of the entire world, ranging from the young child who donates his lemonade stand proceeds to a homeless person down the street to a doctor who provides free medical care to a child in an impoverished country, a lawyer offering free legal advice, someone who gives a few dollars to a stranger experiencing troubled times, religious groups, political and quasi-political groups, a person who donates blood to the blood bank and to a donor bequeathing sums of money to a 501(c) charitable organization in the United States. Virtually any person and entity anytime anywhere, through a seemingly nice gesture to a more formal one, falls under this large umbrella of Objector's "community." In simplest terms, planet Earth is not what the Guidelines would conceive as a delineated community for a generic domain like <.CHARITY>.

Second, how Objector's subset of "charities and charitable institutions" fits within this broad community is unclear, and, even within this subset, the existence of any type of formal or distinct boundaries is wholly lacking. Indeed, Objector is readily transparent about this obvious fact. In prior correspondence with Applicant and in the present Objection, Objector recognizes the essential inability to delineate a community connoted by such a generic, broad and widely-encompassing dictionary word in the English language, conceding the so-called "charity community" is "not institutionalized and straddles the border between different stakeholders of the community of charitable organizations." *See* Objn at 10, ¶ 21. Admitting this subset is "less structured or organized" than other types of communities, it is inconceivable how Objector leaps from this realization to the conclusion that there is a clearly delineated community. *Id.* Indeed Objector himself in another context readily admits that generic words like "charity" cannot meet the clearly delineated test for community. They are too broad and lacking in specifics to meet the necessary requirements set out by ICANN.[1] This is precisely why the standard is written in this manner: so that the Community objection process cannot be used as a weapon to block legitimate uses of generic words that do not describe clearly delineated communities. This analysis applies to other elements below.

Even within the realm of organized and official charitable organizations, on a global scale, there are no overarching rules or associations defining or regulating them. What is required in the United States, for example, to file as a 501(c) entity is not necessarily applicable or even relevant for a charitable or non-profit entity in England, Australia, Canada, Japan, Mexico or any other country around the world.

Third, the word "charity" itself has many meanings: (1) benevolent goodwill toward or love of humanity; (2)(a) generosity and helpfulness especially toward the needy or suffering; also aid given to those in need; (2)(b) an institution engaged in relief of the poor; (2)(c) public provision for the relief of the needy; (3)(a) a gift for public benevolent purposes; (3)(b) an institution (as a hospital) founded by such a gift; (4) lenient judgment of others. *See* http://www.merriam-webster.com/dictionary/charity. In other words, in addition to the word's affiliation with entities and organizations that provide monetary and other relief to those in need, the word itself carries a far broader meaning and context in that it "connotes kindness toward others" and "is a means for expression for those devoted to compassion and good will." Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 7).

Stated another way, "charity" does not denote a "community;" it represents a *subject*. It is a global term that is understood in multiple languages and cultures and describes important services and/or a state of mind. Applicant applied for the TLD name for precisely that purpose. Nevett Dec. ¶ 7 (**Annex B**). For example, the string may be used by entities that are not charities themselves but conduct business with the philanthropic community, rate or comment on charities, or otherwise have legitimate and lawful reasons for interacting with charitable organizations. Neither Applicant nor the public should be constrained from discourse on a subject of such universal relevance. As the Objector admits, the word's

[1] Objector has stated that "as a general remark and because I have reviewed all applications, it is difficult in these cases to prove the existence of a clearly delineated community. By definition, a 'generic term' is a term which is used by a significant number of people, who do not necessarily share similar goals, values or interests. A specific community should distinguish itself from others, precisely by its characteristics or specificities. It cannot be the case for a 'generic term' which, by definition, goes beyond specificities as it is used by very different persons." *See* Letter from ICANN Independent Objector, at "Community Objections" ¶ 4 (**Annex C**).

broad meanings make it impossible for Objector to show that it describes a true community and, put in context of the elements enumerated in the objection standard, Objector does not show that the public recognizes “charity” as a “community.” AGB § 3.5.4 at 3-22, 3-23; *see also* Objn at 10.

Upholding the Objection would stifle expression and discussion concerning this important topic. Such a result would undermine the very purpose of the new gTLD program, and contravenes Applicant’s open-Internet philosophy to benefit the public, increase consumer choice, promote free expression and allow the Internet marketplace to function, grow and innovate. *See* Nevett Dec. ¶¶ 4-6, 8. For such reasons, and because Objector fails to carry his burden to prove a “clearly delineated community,” the Objection cannot succeed.

2. *Objector Demonstrates No Substantial Opposition to the Application Within the “Community” He Claims to Represent.*

Objector must prove “substantial opposition” within the community on whose behalf he purports to speak. The Panel considers a number of factors to determine whether he meets this standard, including: (1) the number of expressions of opposition to the Application relative to the asserted community’s composition; (2) the representative nature of those expressing opposition; (3) the stature or weight of sources of opposition; (4) the distribution or diversity of opposition within the invoked community; (5) Objector’s historical defense of the alleged community in other contexts; and (6) costs incurred by Objector in expressing opposition. AGB § 3.5.4 at 3-23.

The Objection offers virtually no evidence to show any, let alone substantial, opposition. Indeed, Objector admits that the only opposition – expressed through public comments on the ICANN website – comes “mainly . . . from the United Kingdom.” Objn at 12, ¶ 28. The Objection focuses on three public comments made to ICANN along with an Australian GAC Early Warning to support the notion that there is opposition to Applicant’s proposed <.CHARITY> gTLD. *See* Objn at 12. All three of these public comments come from organizations in the UK. Two of them – the Association of Charitable Foundations and the National Council for Voluntary Organisations – share identical language indicating one expression of concern, not two. The other UK public comment – from The Charity Commission for England and Wales – merely points out the general “concern” for consumer confusion and abuse” if the TLD is not administered properly. The comment says nothing about Applicant in particular nor does it provide any suggestion that the security measures Applicant intends to put in place for this TLD would actually increase consumer confusion or abuse. This comment is a reason to examine Applicant’s safeguards (there are many) rather than to attempt to block the new TLD through the objection process. Donuts has worked with many organizations in order to address concerns and describe safeguards.

A careful review of all of the ICANN public comments in connection with Applicant’s <.CHARITY> application reveals that no “substantial opposition” has occurred at all. There are only seven appearing to represent actual charitable organizations or foundations lodging community objection comments (three of which are addressed above in the preceding paragraph). Almost all of them emanate from the UK, share verbatim language and generally repeat the same two concerns: (1) that the <.CHARITY> TLD should be run by a non-profit organization - an argument with which not even Objector agrees; and (2) that <.CHARITY> should be a community-based TLD – something that is not required by ICANN for this gTLD. “Simply not wanting another party to be the applicant or obtain the name is not sufficient to [grant an objection].” See http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv4-12nov10-en.pdf. Both concerns are addressed more fully below in the next section.[2]

[2] Beyond these public comments, the only remaining “opposition” mentioned by Objector is the Early Warning from Australia. Australia, which filed well over 100 Early Warnings and

From only these few public comments along with the GAC Early Warning, Objector proceeds directly to the conclusion that "[e]ven if the opposition has largely emanated from the UK and Australian jurisdictions, concerns voiced are without doubt substantial . . ." Objn at 13, ¶ 33. How one can characterize a few public comments primarily from the UK as opposition from a significant portion of the global "charity community" is puzzling at best. Spatial distribution is a factor enumerated in the standards for both "clearly delineated" and "substantial opposition." While this is not to say that the parties expressing concern must necessarily represent every part of the world in order to be considered – if, for example, the string itself were focused upon a particular area (*e.g.* <.UKcharity>) - the absence of challenges from all but one or less than a handful of countries is highly probative and, in this case, negates any finding of substantial opposition.

Objector has provided none of the type of evidence one might expect to back his position. These would include exhibits in support of opposition, information as to how many alleged members of the purported community join the Objection, a showing of any historical "defense" mounted for the "community" invoked, mention of the distribution or diversity of opposition or evidence of costs incurred. Objector offers not one letter from a single member of the "community" expressing opposition to the <.CHARITY> gTLD. He did not do so, notwithstanding that such information represents just what the Guidebook's elements of "substantial opposition" expressly call for. AGB § 3.5.4 at 3-23. "Evidence is appropriately required in all types of objection proceedings. Absent evidence, no objection should stand." *See* http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf.

The Objector falls well short of showing "substantial opposition" within the community, and the Objection should be rejected. AGB § 3.5.4 at 3-25.

3. Objector Demonstrates No "Strong Association" Between the "Community" Invoked and the Applied-For String.

Objector bears the burden of proving a "strong association" between the applied-for string and the so-called community it invokes. It may do so by showing (1) statements made in the Application; (2) other public statements by Applicant; and (3) public associations between the string and the objecting "community." AGB § 3.5.4 at 3-24.

Applicant intends to offer this gTLD to a wide variety of users. For example, in response to item 18(a) of the Application, seeking "the mission/ purpose of your proposed gTLD," Applicant has stated generally:

> This TLD is attractive and useful to end-users as it better facilitates search, self-expression, information sharing and the provision of legitimate goods and services.
>
> This TLD is a generic term and its second level names will be attractive to a variety of Internet users.
>
> No entity, or group of entities, has exclusive rights to own or register second level names in this TLD.

was the only country to file an Early Warning, did not advocate for the blocking of the <.CHARITY> TLD, but rather that there be appropriate safeguards. If Australia wanted ICANN to reject the application for <.CHARITY> outright there was an opportunity to do so via the GAC Advice procedure, which Australia failed to do. *See* http://www.icann.org/en/news/correspondence/gac-to-board-11apr13-en.

See Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 8). Indeed, targeting a discrete group or community runs directly contrary to Applicant's philosophy behind the Internet and the operation of this and other registries by its family of companies:

> Making this TLD available to a broad audience of registrants is consistent with the competition goals of the New TLD expansion program, and consistent with ICANN's objective of maximizing Internet participation. Donuts believes in an open Internet and, accordingly, we will encourage inclusiveness in the registration policies for this TLD. In order to avoid harm to legitimate registrants, Donuts will not artificially deny access, on the basis of identity alone (without legal cause), to a TLD that represents a generic form of activity and expression.

Id. While Applicant references those "organizations that collect and distribute funds and materials for charities, provide for individuals and groups with medical or other special needs, and raise awareness for issues and conditions that would benefit from additional resources," its application makes clear that it ultimately intends the domain "will be of interest to the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need." *Id.* The application establishes that "the term CHARITY, which connotes kindness towards others, is a means for expression for those devoted to compassion and good will." *Id.* The application in no way specifically "targets" non-profit charitable organizations.

In addition, Objector presents no evidence that the *public* "strongly associates" the word "charity" with any delineated community. Objector concludes that "the term 'charity' is generally associated in the public mind with giving for what is seen as a good cause, and likewise with not for profit institutions." Objn at 8, ¶ 13. He suggests that the string, therefore, targets this subset of charitable organizations. This, however, does not bolster the position that targeting is present. Rather, it identifies users who may have an interest in the subject of charity, which, as described, includes essentially the entire world population – hardly a "community."

As Objector states, "a 'generic term' is a term which is used by a significant number of people, who do not necessarily share similar goals, values or interests. A specific community should distinguish itself from others, precisely by its characteristics or specificities. It cannot be the case for a 'generic term' which, by definition, goes beyond specificities as it is used by very different persons." *See* Letter from ICANN Independent Objector, at "Community Objections" ¶ 4 (**Annex C**). There can be no strong association between the string and "Community" for a generic word.

Moreover, as shown above, the Application goes beyond that universe of end users to include those more generally interested in "self-expression, information sharing and the provision of legitimate goods and services," and notes that, as a generic term, the TLD and "its second level names will be attractive to a variety of Internet users." Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 8).

Objector's unsubstantiated conclusions regarding the string does nothing to prove a "strong" association between it and the subset of narrow interests for which Objector claims he seeks protection. This should come as no surprise, given the broad meaning of the term. As such, the Objection must fail. AGB at 3-24.

4. Objector Does Not Prove Material Detriment.

Just as critically – and likewise dispositively – Objector cannot sustain his burden to prove "likelihood" of "material detriment." That independently required factor calls for proof of the following elements: (1) the nature and extent of potential damage to the invoked "community" or its reputation from Applicant's operation of the string; (2) evidence that

Applicant does not intend to act consistent with the interests of the invoked community; (3) interference with the core activities of the invoked community by Applicant's operation of the string; (4) extent the invoked community depends on the DNS for core activities; and (5) the level of certainty that detrimental outcomes will occur. AGB § 3.5.4 at 3-24.

Objector provides no *evidence* to establish *any* of these elements.[3] Although he makes several separate arguments, a close review of the Objection demonstrates that Objector raises only one point –that is, if the <.CHARITY> TLD is made available to those beyond recognized non-profit charitable organizations, abuse and harm may occur. While agreeing with Applicant that the <.CHARITY> gTLD need not be *run* by a non-profit organization (Objn at 15, ¶ 40), Objector finds it "striking that the Application has not been framed … as a community-based gTLD" (Objn at 15, ¶ 42) and he mirrors the public comments in this regard to suggest that those seeking to register domains under this TLD be limited only to non-profit organizations. These comments conclude that a <.CHARITY> gTLD should be run similar to the <.ORG> TLD. Objector reasons that the ""charity' brand largely operates on the basis of trust" and creating strict eligibility requirements by limiting the TLD only to non-profits would somehow avoid exacerbated abuse and fraud. *See* Objn at 14, ¶¶ 38, 39.

This argument raised in the public comments and embraced by Objector that <.CHARITY> should be limited to non-profit charitable organizations similar to the <.ORG> TLD is overly simplistic and is not relevant toward proving detriment. The <.ORG> TLD, which historically was operated by a for-profit entity and now managed by Public Interest Registry, does not limit itself to non-profit organizations and is not restricted to any one category of registrants. *See, e.g.,* http://www.pir.org/about/history.

Even more, ICANN, does not require an operator to apply as a community. "The ultimate goal of the community-objection process is to prevent the misappropriation of a community label by delegation of a TLD and to ensure that an objector cannot keep an applicant with a legitimate interest in the TLD from succeeding." *See* http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf). Virtually any generic term could potentially be argued to implicate a "community," as Objector does here. Allowing so-called community interests to stifle expression, restrain competition and impede growth in the namespace would defeat the very purpose of the new gTLD program. Nor does the choice *not* to seek community status constitute *proof* of *harm*. Objector *conjectures* that harm *may* occur due to what he sees as a lack of mechanisms for the proposed TLD to protect the alleged community to the extent he deems necessary. The overwhelming facts convincingly show otherwise.

In fact, Applicant shares the Objector's desire for the <.CHARITY> gTLD to be used for the "creation of a trusted place of information" about charitable activities and has taken proactive steps on this front. Applicant has expressed its affirmative intent to act in the best interests of and to protect all users, including asserted communities, and to "make this TLD a place for Internet users that is far safer than existing TLDs." Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 8). It will do so with 14 protections that ICANN demands for new gTLDs (but has never required for existing gTLDs). Nevett Dec. ¶ 9, Ex. 1 at 8-9 (**Annex B**). Moreover, for this and all its applications, Donuts goes beyond these measures to implement eight additional safeguards, including to address the exact types of concerns raised by Objector. *Id.* ¶ 11, Ex. 1 at 8 (**Annex B**).

Significantly, with respect to the <.CHARITY> Domain and others deemed potentially *sensitive*, Applicant has taken four additional steps to shield users from potential misconduct. *See* Nevett Dec. ¶ 12 (**Annex B**). These include: (i) more frequent and extensive Whois data

[3] "Evidence is appropriately required in all types of objection proceedings. Absent evidence, no objection should stand." *See* http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf.

verification and enhanced take-down processes; (ii) exclusion of registrars with poor compliance history; (iii) regular affirmative registry monitoring for fraud and other forms of misconduct; and (iv) requiring elevated security measures by registrars. *Id*.

Objector obtusely suggests a need for registration eligibility criteria, although without proposing what they might be. Existing gTLDs, including <.ORG>, have no such requirement. And, the very term "charity" about which Objector complains here appears more than 14,000 times in second-level domains. Nevett Dec. ¶ 17 (**Annex B**). Applicant has clearly stated its opposition to such constraints on access, expression and innovation:

> [A]ttempts to limit abuse by limiting registrant eligibility is unnecessarily restrictive and harms users by denying access to many legitimate registrants. Restrictions on second level domain eligibility would prevent law-abiding individuals and organizations from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD.

Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 8). ICANN supports the same objectives. Indeed, they lie at the heart of the entire new gTLD program. *See*, *e.g.*, AGB Preamble, § 1.1.2.3, and Mod. 2 Attmt. at A-1.

There are two separate applicants for the <.CHARITY> gTLD. By trying to exclude both applicants, Objector would effectively knock out the TLD in its entirety, thereby causing material harm to the purported community, as that would in turn mean that no one would operate it. A few letters from some charitable organizations in the UK is hardly a reason to restrict freedom of expression from all around the world. There would be no greater example of censorship.

The Objection would have the Panel gut these principles in deference to the self-interest of Objector and its theoretical community. This would subvert the goals of the evaluation process and lead the namespace down a dangerous path. Such censorship has no place on the Internet. Applicant's content-neutral approach strikes the proper balance that promotes free speech and the growth of cyber media, while protecting users more thoroughly than both the current landscape and ICANN's new gTLD enhancements do.

Objector's lament that Applicant's proposal lacks sufficient means to combat misconduct or protect user interest simply has no basis in fact. In light of such sweeping and unprecedented undertakings, Applicant finds it difficult to imagine what more it could do or Objector could want.

Objector fails to establish any of the Guidebook's remaining elements of detriment. He does not show interference with the "core activities" of any charity "community," or that it "depends" on the domain name system for such "activities." And he does not venture an assessment of "certainty" of harm. Objector's fears and rank speculation do not satisfy his burden to prove that harm is "likely" from Applicant's operation of the truly generic TLD at issue. The Objection must fail.

Applicant has every right to full consideration of its Application by ICANN. Objector fails in every respect to meet its burden to divest Applicant of that right. The Objection cannot succeed. Applicant therefore respectfully urges the Panel to reject it and to direct Objector to pay the costs reasonably incurred by Applicant in opposing the Objection.

Communication (Article 6(a) of the Procedure and Article 1 of the ICC Practice Note)

A copy of this Response is/was transmitted to the Objector on June 6, 2013
by email to the following addresses Contact Information Redacted
Contact Information Redacted

A copy of this Response is/was transmitted to ICANN on June 6, 2013 by e-mail to the following address: DRfiling@icann.org.

Filing Fee (Article 1 Appendix III to the Rules and Article 11(f) of the Procedure)

As required, Euros 5 000 were paid to ICC on May 15, 2013.

□ Evidence of the payment is attached for information.

Description of the Annexes filed with the Response (Article 11(e) of the Procedure)
List and Provide description of any annex filed.

Annex A – Table of Defined Terms

Annex B – Declaration of Jonathon Nevett, with the following exhibits:

Exhibit 1 – Application ID 1-1384-49318 for <.charity> gTLD by Corn Lake, LLC

Exhibit 2 – List of new gTLDs applied for by Donuts Inc. companies

Annex C – Letter from ICANN Independent Objector

DATED: June 6, 2013

Respectfully submitted,

THE IP & TECHNOLOGY LEGAL GROUP, P.C.
dba New gTLD Disputes

By: _____/jmg/____________
John M. Genga
Contact Information Redacted

By: _____/dcm/____________
Don C. Moody
Contact Information Redacted

Attorneys for Applicant/Respondent
CORN LAKE, LLC

Annex A

Table of Defined Terms

ANNEX A

Table of Defined Terms

Abbreviation	**Reference**
"ICANN"	Internet Corporation for Assigned Names and Numbers
"Guidebook" or "AGB"	The gTLD Applicant Guidebook, approved by ICANN on June 20, 2011, and as updated on January 11 and June 4, 2012
"ICC"	International Chamber of Commerce
"TLD" or "string"	A top level domain, also referred to as a "string" by ICANN – *e.g.*, Guidebook §§ 3.2.1, 3.5.4
"Objector" or "IO"	Prof. Alain Pellet, Independent Objector
"Applicant" or "Respondent"	Corn Lake, LLC
"Donuts"	Donuts Inc., ultimate parent of Applicant
"Application"	Applicant's application ID no. 1-1384-49318 for the <.CHARITY> TLD
"Objection"	The objection to the Application submitted to the ICC by Objector on March 13, 2013
"Response"	Applicant's response to the Objection, of which this **Annex A** is a part
"Panel"	ICC's appointee to consider and rule upon the Objection

Annex B

Declaration of J. Nevett

DECLARATION OF JONATHON NEVETT

I, Jonathon Nevett, declare as follows:

1. I am a founder and Executive Vice President of Donuts Inc., the ultimate parent of Corn Lake, LLC ("Applicant" or "Respondent"). Applicant has filed Application No. ID 1-1384-49318 (the "Application") for the generic top-level domain ("gTLD") <.charity> (at times herein, the "Domain"). A true, correct and complete copy of the public portion of the Application is attached hereto as **Exhibit 1**.

2. I had close involvement with the Application process and, as described below, with the new gTLD program formulated by the Internet Corporation for Assigned Names and Numbers ("ICANN"). As such, I have personal knowledge of the matters set forth in this declaration. I make this declaration in support of Respondent's opposition to the objection to the Application ("Objection") filed by Prof. Alain Pellet, Independent Objector ("Objector").

Donuts' Background

3. I and the rest of Donuts' management have decades of combined experience in the domain name business, as accurately reflected in our biographies on Donuts' website, http://donuts.co/index.php?option=com_content&view=article&id=8&Itemid=105. We formed Donuts to acquire and operate new generic top-level domains under ICANN's new gTLD program that launched officially in July 2011. I and others in our management team have been involved with and provided input to help craft that program as far back as 2004, as part of ICANN's multiple stakeholder process that involved constituencies such as governments, business and intellectual property stakeholders, and technologists. Formation of the program included, for example, creating standards for gTLD applicants, designing protection mechanisms for intellectual property rights-holders, and conferring with industry colleagues on the economic impact of new gTLDs.

New gTLD Objectives and Donuts' Philosophy

4. From my own involvement, I understand that ICANN developed the new gTLD program to increase competition and choice in the domain name space. Indeed, the top of the

"About" page of its new gTLD website, http://newgtlds.icann.org/en/about/program, expressly so states. I also understand that the program's intent includes the promotion of free expression, as supported by statements in ICANN's new gTLD Applicant Guidebook ("Guidebook") – *e.g.*, "everyone has the right to freedom of expression," Guidebook at 3-21.

5. Donuts joins in these aims. Through subsidiary entities such as Applicant, it has applied for 307 new gTLDs. A complete and correct list of all new gTLDs applied for by Donuts entities is attached hereto as **Exhibit 2**. These applications, along with approximately 1,600 submitted by others to ICANN, *see* http://newgtlds.icann.org/en/program-status/statistics, will create competition among domain name registries that has not previously existed in a landscape that has had only 22 gTLDs to this point, http://newgtlds.icann.org/en/program-status/application-results/strings-1200utc-13jun12-en. Such competition advances the program's goals, shared by Donuts, to expand consumer choice in the name space.

6. Donuts has adopted a business model that it believes enhances consumer choice more effectively than it could have achieved with a lesser number of applied-for names. By applying for and scaling up to run a large number of new gTLDs, Donuts achieves economies of scale that allow it to offer domains representing terms and subjects that otherwise could not be brought to the name space economically and, consequently, would not have their own forum. In the way of analogy, Donuts views <.com> as a large downtown "department store" that has not had much competition. Instead of competing with <.com> by building another department store a few blocks away, Donuts' idea is to create a "shopping mall" environment that allows for "boutiques" to share the expanding mall space. By doing so, Donuts can provide more consumer choice and specificity in the domain name space.

Donuts' Selection and Proposed Operation of Its Applied-for gTLDs

7. The 307 gTLDs for which Donuts applied were carefully selected as subject areas that Donuts believes will interest Internet users and involve them in the domain. Donuts deliberately chose common words from the dictionary so that consumers could make use of the

gTLDs in accordance with the meanings they ascribe to those words. In no case did Donuts opt for a generic term *because* it also denotes an industry group in other contexts. Indeed, we understand that dictionary terms commonly can identify subjects that include commercial interests. We studied various data sources, built and utilized algorithms, and relied on our various industry experiences in determining which names to apply for.

8. Donuts also believes that consumer choice and innovation in the name space depend significantly on freedom of expression. Donuts forthrightly voices that philosophy in its response to question 18(a) of all its applications, as follows:

> This TLD is attractive and useful to end-users as it better facilitates search, self-expression, information sharing and the provision of legitimate goods and services. Along with the other TLDs in the Donuts family, this TLD will provide Internet users with opportunities for online identities and expression that do not currently exist. In doing so, the TLD will introduce significant consumer choice and competition to the Internet namespace – the very purpose of ICANN's new TLD program.
>
> This TLD is a generic term and its second level names will be attractive to a variety of Internet users. Making this TLD available to a broad audience of registrants is consistent with the competition goals of the New TLD expansion program, and consistent with ICANN's objective of maximizing Internet participation. Donuts believes in an open Internet and, accordingly, we will encourage inclusiveness in the registration policies for this TLD. In order to avoid harm to legitimate registrants, Donuts will not artificially deny access, on the basis of identity alone (without legal cause), to a TLD that represents a generic form of activity and expression.

9. From participating in the development of the new gTLD program, Donuts also understands that the significant expansion resulting from it raised concerns among stakeholders

for preserving the rights of others and protecting users from misconduct. These concerns led Donuts to support and ICANN to oblige new gTLD applicants to take 14 additional actions that existing gTLDs do not. Applicant enumerates and commits to implementing each such requirement in response to question 18(a) of all its applications.

10. Such new measures are designed to maximize the ability of the registry to address issues quickly and effectively if and when they arise. Consistent with the objectives of the program, the new requirements do not seek to prevent potential problems by denying access to users. Donuts agrees with this approach as well, stating in its applications:

> No entity, or group of entities, has exclusive rights to own or register second level names in this TLD. There are superior ways to minimize the potential abuse of second level names, and in this application Donuts will describe and commit to an extensive array of protections against abuse, including protections against the abuse of trademark rights.
>
> We recognize some applicants seek to address harms by constraining access to the registration of second level names. However, we believe attempts to limit abuse by limiting registrant eligibility is unnecessarily restrictive and harms users by denying access to many legitimate registrants. Restrictions on second level domain eligibility would prevent law-abiding individuals and organizations from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD. As detailed throughout this application, we have struck the correct balance between consumer and business safety, and open access to second level names.

11. To maintain access as open as possible, Donuts voluntarily committed in its applications to taking eight *more* protective steps, *in addition to* the 14 that ICANN *already* has imposed *over and above* what it demands of existing gTLD operators. These are:

1. Periodic audit of Whois data for accuracy;

2. Remediation of inaccurate Whois data, including takedown, if warranted;

3. A new Domain Protected Marks List (DPML) product for trademark protection;

4. A new Claims Plus product for trademark protection;

5. Terms of use that prohibit illegal or abusive activity;

6. Limitations on domain proxy and privacy service;

7. Published policies and procedures that define abusive activity; and

8. Proper resourcing for all of the functions above.

These tools provide tangible safeguards that simply do not exist within most existing gTLDs. Among other things:

- Whois audits and takedown procedures allow for verification of registrant identity and the right to take action against fraudulent registrant.
- Terms of use and published policies also permit Donuts to act in situations where existing registries either refuse or have no right to do so.
- Donuts' DPML and Claims Plus process, combined with the ICANN-required safeguards, including the Uniform Rapid Suspension (URS) process (the initial recommendation of which I co-authored) offer unprecedented protections to trademark owners that will help them police and take action against misuse of their marks online.
- The "resourcing" Donuts will provide to implement these measures includes a compliance staff dedicated full-time to address such issues.

All of these measures add security to Donuts' domains without restricting initial access to them and potentially quashing legitimate expression in and uses of the name space.

12. Further, as to this Domain and others deemed potentially sensitive, Donuts has taken four additional steps to shield users from potential misconduct. These include: (i) more frequent and extensive Whois data verification and enhanced take-down processes; (ii)

exclusion of registrars with poor compliance history; (iii) regular affirmative registry monitoring for fraud and other forms of misconduct; and (iv) requiring elevated security measures by registrars.

13. In addition, Donuts has made Public Interest Commitments (PICs) as to *all* of its 307 strings. The PICs lay out specific undertakings on the part of Donuts to benefit and protect the interests of users, rights holders and others. Further, they make such commitments contractually binding so as to allow ICANN to terminate any Donuts registry that does not honor its PICs.

14. Finally, Donuts has passed ICANN's background screening process for about 95 of its 307 applications to date. (ICANN is screening its more than 1,900 applications in an order established by a random drawing that took place several months ago.) Thus, ICANN has determined that Donuts is amply fit to operate a registry.

Donuts' Investment

15. Through subsidiary entities, such as Applicant, Donuts has applied for 307 new gTLDs. This represents by far the greatest number of applications made for new gTLDs by any applicant, Google being second with 101 and Amazon third with 78.

16. With the ICANN fee of $185,000 per application, Donuts has invested nearly $57 million simply to file its new gTLD applications. It has invested millions more for technical and other support to operate the registries for those gTLDs if and when issued them. It has not done so lightly or with anything less than the highest standards for dependable operation, open access and effective security. Not meeting its own expectations would not merely compromise its ideals; such failure would also harm its business. Donuts has not raised well over a hundred million dollars to do a poor job and lose its investors' considerable capital.

Matters Raised by the Instant Objection

17. In response to the Objection's accusations that the Domain may somehow harm an alleged community, I note that Donuts has sought to determine the extent to which "charity" appears at the second level in six existing TLDs – <.com>, <.org>, <.net>, <.info>, <.biz> and

<.us>. I directed this survey and know how it was done. Each of these registries must publish a "zone file," listing each of the second level domain names contained in each registry (e.g., there are in excess of 110 million second level names in <.com>). By analyzing these "zone files", we uncovered 14,257 uses of the term "charity" at the second level of the six investigated TLDs.

I declare under penalty of perjury under the laws of the United States that based on my knowledge and belief the foregoing is true and correct and that this declaration was executed by me on June 6, 2013, in Rockville, Maryland, USA.

/jn/
Jonathon Nevett

Annex B - Exhibit 1

Applicant’s gTLD Application for <.CHARITY>

New gTLD Application Submitted to ICANN by: Corn Lake, LLC

String: charity

Originally Posted: 13 June 2012

Application ID: 1-1384-49318

Applicant Information

1. Full legal name

Corn Lake, LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

+1 425 671 0020

5. If applicable, website or URL

Primary Contact

6(a). Name

Daniel Schindler

6(b). Title

EVP, Donuts Inc.

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Jonathon Nevett

7(b). Title

EVP, Donuts Inc.

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Delaware. http://delcode.delaware.gov/title6/c018/sc01/index.shtml

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

Dozen Donuts, LLC

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

11(b). Name(s) and position(s) of all officers and partners

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

Dozen Donuts, LLC	N/A

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Paul Stahura	CEO, Donuts Inc.

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

charity

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. 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.

Donuts has conducted technical analysis on the applied-for string, and concluded that there are no known potential operational or rendering issues associated with the string.

The following sections discuss the potential operational or rendering problems that can arise, and how Donuts mitigates them.

## Compliance and Interoperability

The applied-for string conforms to all relevant RFCs, as well as the string requirements set forth in Section 2.2.1.3.2 of the Applicant Guidebook.

## Mixing Scripts

If a domain name label contains characters from different scripts, it has a higher likelihood of encountering rendering issues. If the mixing of scripts occurs within the top-level label, any rendering issue would affect all domain names registered under it. If occurring within second level labels, its ill-effects are confined to the domain names with such labels.

All characters in the applied-for gTLD string are taken from a single script. In addition, Donuts’s IDN policies are deliberately conservative and compliant with the ICANN Guidelines for the Implementation of IDN Version 3.0. Specifically, Donuts does not allow mixed-script labels to be registered at the second level, except for languages with established orthographies and conventions that require the commingled use of multiple scripts, e.g. Japanese.

## Interaction Between Labels

Even with the above issue appropriately restricted, it is possible that a domain name composed of labels with different properties such as script and directionality may introduce unintended rendering behaviour.

Donuts adopts a conservative strategy when offering IDN registrations. In particular, it ensures that any IDN language tables used for offering IDN second level registrations involve only scripts and characters that would not pose a risk when combined with the top level label.

## Immature Scripts

Scripts or characters added in Unicode versions newer than 3.2 (on which IDNA2003 was based) may encounter interoperability issues due to the lack of software support.

Donuts does not currently plan to offer registration of labels containing such scripts or characters.

## Other Issues

To further contain the risks of operation or rendering problems, Donuts currently does not offer registration of labels containing combining characters or characters that require IDNA contextual rules handling. It may reconsider this decision in cases where a language has a clear need for such characters.

Donuts understands that the following may be construed as operational or rendering issues, but considers them out of the scope of this question. Nevertheless, it will take reasonable steps to protect registrants and Internet users by working with vendors and relevant language communities to mitigate such issues.

- missing fonts causing string to fail to render correctly; and
- universal acceptance of the TLD;

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

Q18A SV CHAR: 7846

ABOUT DONUTS
Donuts Inc. is the parent applicant for this and multiple other TLDs. The company intends to increase competition and consumer choice at the top level. It will operate these carefully selected TLDs safely and securely in a shared resources

business model. To achieve its objectives, Donuts has recruited seasoned executive management with proven track records of excellence in the industry. In addition to this business and operational experience, the Donuts team also has contributed broadly to industry policymaking and regulation, successfully launched TLDs, built industry-leading companies from the ground up, and brought innovation, value and choice to the domain name marketplace.

ABOUT DONUTS’ RESOURCES
Donuts’ has raised more than US$100 million from a number of capital sources for TLDs. Our well-resourced, capable and skilled organization will operate these TLDs and benefit Internet users by:

1. Providing the operational and financial stability necessary for TLDs of all sizes, but particularly for those with smaller volume (which are more likely to succeed within a shared resources model);
2. Competing more powerfully against incumbent gTLDs; and
3. More thoroughly and uniformly executing consumer and rights holder protections.

THE .CHARITY TLD
This TLD is attractive and useful to end-users as it better facilitates search, self-expression, information sharing and the provision of legitimate goods and services. Along with the other TLDs in the Donuts family, this TLD will provide Internet users with opportunities for online identities and expression that do not currently exist. In doing so, the TLD will introduce significant consumer choice and competition to the Internet namespace – the very purpose of ICANN’s new TLD program.

This TLD is a generic term and its second level names will be attractive to a variety of Internet users. Making this TLD available to a broad audience of registrants is consistent with the competition goals of the New TLD expansion program, and consistent with ICANN’s objective of maximizing Internet participation. Donuts believes in an open Internet and, accordingly, we will encourage inclusiveness in the registration policies for this TLD. In order to avoid harm to legitimate registrants, Donuts will not artificially deny access, on the basis of identity alone (without legal cause), to a TLD that represents a generic form of activity and expression.

The .CHARITY TLD will be of interest to the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need. This broad and diverse set includes organizations that collect and distribute funds and materials for charities, provide for individuals and groups with medical or other special needs, and raise awareness for issues and conditions that would benefit from additional resources. In addition, the term CHARITY, which connotes kindness toward others, is a means for expression for those devoted to compassion and good will. We would operate the .CHARITY TLD in the best interest of registrants who use the TLD in varied ways, and in a legitimate and secure manner.

DONUTS’ APPROACH TO PROTECTIONS
No entity, or group of entities, has exclusive rights to own or register second level names in this TLD. There are superior ways to minimize the potential abuse of second level names, and in this application Donuts will describe and commit to an extensive array of protections against abuse, including protections against the abuse of trademark rights.

We recognize some applicants seek to address harms by constraining access to the registration of second level names. However, we believe attempts to limit abuse by limiting registrant eligibility is unnecessarily restrictive and harms users by denying access to many legitimate registrants. Restrictions on second level domain eligibility would prevent law-abiding individuals and organizations from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD. As detailed throughout this application, we have struck the correct balance between consumer and business safety, and open access to second level names.

By applying our array of protection mechanisms, Donuts will make this TLD a place for Internet users that is far safer than existing TLDs. Donuts will strive to operate this TLD with fewer incidences of fraud and abuse than occur in incumbent TLDs. In addition, Donuts commits to work toward a downward trend in such incidents.

OUR PROTECTIONS
Donuts has consulted with and evaluated the ideas of international law enforcement, consumer privacy advocacy organizations, intellectual property interests and other Internet industry groups to create a set of protections that far exceed those in existing TLDs, and bring to the Internet namespace nearly two dozen new rights and protection mechanisms to raise user safety and protection to a new level.

These include eight, innovative and forceful mechanisms and resources that far exceed the already powerful protections in the applicant guidebook. These are:

1. Periodic audit of WhoIs data for accuracy;
2. Remediation of inaccurate Whois data, including takedown, if warranted;
3. A new Domain Protected Marks List (DPML) product for trademark protection;
4. A new Claims Plus product for trademark protection;
5. Terms of use that prohibit illegal or abusive activity;
6. Limitations on domain proxy and privacy service;
7. Published policies and procedures that define abusive activity; and
8. Proper resourcing for all of the functions above.

They also include fourteen new measures that were developed specifically by ICANN for the new TLD process. These are:

1. Controls to ensure proper access to domain management functions;
2. 24⁄7⁄365 abuse point of contact at registry;
3. Procedures for handling complaints of illegal or abusive activity, including remediation and takedown processes;
4. Thick WhoIs;
5. Use of the Trademark Clearinghouse;
6. A Sunrise process;
7. A Trademark Claims process;
8. Adherence to the Uniform Rapid Suspension system;
9. Adherence to the Uniform Domain Name Dispute Resolution Policy;
10. Adherence to the Post Delegation Dispute Resolution Policy;
11. Detailed security policies and procedures;
12. Strong security controls for access, threat analysis and audit;
13. Implementation DNSSEC; and
14. Measures for the prevention of orphan glue records.

Due to the level of end-user trust potentially associated with this string, and consistent with the requirements of Question 30, Donuts will employ these additional four, protections:

1. For this string, to supplement the periodic audit documented above, a deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes.
2. Exclusion of registrars with a history of poor compliance;

3. Regular monitoring by the registry of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes; and
4. In addition to registry-based procedures, requirements that registrars have a 24⁄7⁄365 abuse contact, and remediation and takedown processes.

DONUTS’ INTENTION FOR THIS TLD
As a senior government authority has recently said, “a successful applicant is entrusted with operating a critical piece of global Internet infrastructure.” Donuts’ plan and intent is for this TLD to serve the international community by bringing new users online through opportunities for economic growth, increased productivity, the exchange of ideas and information and greater self-expression.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

Q18B SV CHAR: 8719

DONUTS’ PLACE WITHIN ICANN’S MISSION

ICANN and the new TLD program share the following purposes:
1. To make sure that the Internet remains as safe, stable and secure as possible, while
2. Helping to ensure there is a vibrant competitive marketplace to efficiently bring the benefits of the namespace to registrants and users alike.

ICANN harnesses the power of private enterprise to bring forth these public benefits. While pursuing its interests, Donuts helps ICANN accomplish its objectives by:

1. Significantly widening competition and choice in Internet identities with hundreds of new top-level domain choices;
2. Providing innovative, robust, and easy-to-use new services, names and tools for users, registrants, registrars, and registries while at the same time safeguarding the rights of others;
3. Designing, launching, and securely operating carefully selected TLDs in multiple languages and character sets; and
4. Providing a financially robust corporate umbrella under which its new TLDs will be protected and can thrive.

ABOUT DONUTS’ RESOURCES
Donuts’ financial resources are extensive. The company has raised more than US$100 million from a number of capital sources including multiple multi-billion dollar venture capital and private equity funds, a top-tier bank, and other well-capitalized investors. Should circumstances warrant, Donuts is prepared to raise additional funding from current or new investors. Donuts also has in place pre-funded, Continued Operations Instruments to protect future registrants. These resource commitments mean Donuts has the capability and intent to launch, expand and operate its TLDs in a secure manner, and to properly protect Internet users and rights-holders from potential abuse.

Donuts firmly believes a capable and skilled organization will operate multiple TLDs and benefit Internet users by:

1. Providing the operational and financial stability necessary for TLDs of all sizes, but particularly for those with smaller volume (which are more likely to succeed within a shared resources and shared services model);
2. Competing more powerfully against incumbent gTLDs; and
3. More thoroughly and uniformly executing consumer and rights holder protections.

Donuts will be the industry leader in customer service, reputation and choice. The reputation of this, and other TLDs in the Donuts portfolio, will be built on:
1. Our successful launch and marketplace reach;
2. The stability of registry operations; and
3. The effectiveness of our protection mechanisms.

THE GOAL OF THIS TLD

This and other Donuts TLDs represent discrete segments of commerce and human interest, and will give Internet users a better vehicle for reaching audiences. In reviewing potential strings, we deeply researched discrete industries and sectors of human activity and consulted extensive data sources relevant to the online experience. Our methodology resulted in the selection of this TLD – one that offers a very high level of user utility, precision in content delivery, and ability to contribute positively to economic growth.

SERVICE LEVELS

Donuts will endeavor to provide a service level that is higher than any existing TLD. Donuts' commitment is to meet and exceed ICANN-mandated availability requirements, and to provide industry-leading services, including non-mandatory consumer and rights protection mechanisms (as described in answers to Questions 28, 29, and 30) for a beneficial customer experience.

REPUTATION

As noted, Donuts management enjoys a reputation of excellence as domain name industry contributors and innovators. This management team is committed to the successful expansion of the Internet, the secure operation of the DNS, and the creation of a new segment of the web that will be admired and respected.

The Donuts registry and its operations are built on the following principles:

1. More meaningful product choice for registrants and users;
2. Innovative services;
3. Competitive pricing; and
4. A more secure environment with better protections.

These attributes will flow to every TLD we operate. This string's reputation will develop as a compelling product choice, with innovative offerings, competitive pricing, and safeguards for consumers, businesses and other users.

Finally, the Donuts team has significant operational experience with registrars, and will collaborate knowledgeably with this channel to deliver new registration opportunities to end-users in way that is consistent with Donuts principles.

NAMESPACE COMPETITION

This TLD will contribute significantly to the current namespace. It will present multiple new domain name alternatives compared to existing generic and country code

TLDs. The DNS today offers very limited addressing choices, especially for registrants who seek a specific identity.

INNOVATION

Donuts will provide innovative registration methods that allow registrants the opportunity to secure an important identity using a variety of easy-to-use tools that fit individual needs and preferences.

Consistent with our principle of innovation, Donuts will be a leader in rights protection, shielding those that deserve protection and not unfairly limiting or directing those that don’t. As detailed in this application, far-reaching protections will be provided in this TLD. Nevertheless, the Donuts approach is inclusive, and second level registrations in this TLD will be available to any responsible registrant with an affinity for this string. We will use our significant protection mechanisms to prevent and eradicate abuse, rather than attempting to do so by limiting registrant eligibility.

This TLD will contribute to the user experience by offering registration alternatives that better meet registrants’ identity needs, and by providing more intuitive methods for users to locate products, services and information. This TLD also will contribute to marketplace diversity, an important element of user experience. In addition, Donuts will offer its sales channel a suite of innovative registration products that are inviting, practical and useful to registrants.

As noted, Donuts will be inclusive in its registration policies and will not limit registrant eligibility at the second level at the moment of registration. Restricting access to second level names in this broadly generic TLD would cause more harm than benefit by denying domain access to legitimate registrants. Therefore, rather than artificially limiting registrant access, we will control abuse by carefully and uniformly implementing our extensive range of user and rights protections.

Donuts will not limit eligibility or otherwise exclude legitimate registrants in second level names. Our primary focus will be the behavior of registrants, not their identity.

Donuts will specifically adhere to ICANN-required registration policies and will comply with all requirements of the Registry Agreement and associated specifications regarding registration policies. Further, Donuts will not tolerate abuse or illegal activity in this TLD, and will have strict registration policies that provide for remediation and takedown as necessary.

Donuts TLDs will comply with all applicable laws and regulations regarding privacy and data protection. Donuts will provide a highly secure registry environment for registrant and user data (detailed information on measures to protect data is available in our technical response).

Donuts will permit the use of proxy and privacy services for registrations in this TLD, as there are important, legitimate uses for such services (including free speech rights and the avoidance of spam). Donuts will limit how such proxy and privacy services are offered (details on these limitations are provided in our technical response). Our approach balances the needs of legitimate and responsible registrants with the need to identify registrants who illegally use second level domains.

Donuts will build on ICANN’s outreach and media coverage for the new TLD Program and will initiate its own effort to educate Internet users and rights holders about the launch of this TLD. Donuts will employ three specific communications efforts. We will:

1. Communicate to the media, analysts, and directly to registrants about the Donuts enterprise.
2. Build on existing relationships to create an open dialogue with registrars about what to expect from Donuts, and about the protections required by any registrar selling this TLD.
3. Communicate directly to end-users, media and third parties interested in the attributes and benefits of this TLD.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

Q18C Standard CHAR: 1440

Generally, during the Sunrise phase of this TLD, Donuts will conduct an auction if there are two or more competing applications from validated trademark holders for the same second level name. Alternatively, if there is a defined trademark classification reflective of this TLD, Donuts may give preference to second-level applicants with rights in that classification of goods and services. Post-Sunrise, requests for registration will generally be on a first-come, first-served basis.

Donuts may offer reduced pricing for registrants interested in long-term registration, and potentially to those who commit to publicizing their use of the TLD. Other advantaged pricing may apply in selective cases, including bulk purchase pricing.

Donuts will comply with all ICANN-related requirements regarding price increases: advance notice of any renewal price increase (with the opportunity for existing registrants to renew for up to ten years at their current pricing); and advance notice of any increase in initial registration pricing.

The company does not otherwise intend, at this time, to make contractual commitments regarding pricing. Donuts has made every effort to correctly price its offerings for end-user value prior to launch. Our objective is to avoid any disruption to our customers after they have registered. We do not plan or anticipate significant price increases over time.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

Q22 CHAR: 4979

As previously discussed (in our response to Q18: Mission ⁄ Purpose) Donuts believes in an open Internet. Consistent with this we also believe in an open DNS, where second level domain names are available to all registrants who act responsibly.

The range of second level names protected by Specification 5 of the Registry Operator contract is extensive (approx. 2,000 strings are blocked). This list resulted from a lengthy process of collaboration and compromise between members of the ICANN community, including the Governmental Advisory Committee. Donuts believes this list represents a healthy balance between the protection of national naming interests and free speech on the Internet.

Donuts does not intend to block second level names beyond those detailed in Specification 5. Should a geographic name be registered in this TLD and used for illegal or abusive activity Donuts will remedy this by applying the array of protections implemented in this TLD. (For details about these protections please see our responses to Questions 18, 28, 29 and 30).

Donuts will strictly adhere to the relevant provisions of Specification 5 of the New gTLD Agreement. Specifically:

1. All two-character labels will be initially reserved, and released only upon agreement between Donuts and the relevant government and country code manager.
2. At the second level, country and territory names will be reserved at the second and other levels according to these standards:
2.1. Short form (in English) of country and territory names documented in the ISO 3166-1 list;
2.2. Names of countries and territories as documented by 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
2.3. The list of United Nations member states in six official UN languages, as prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.
Donuts will initially reserve country and territory names at the second level and at all other levels within the TLD. Donuts supports this requirement by using the following internationally recognized lists to develop a comprehensive master list of all geographic names that are initially reserved:

1. The short form (in English) of all country and territory names contained on the ISO 3166-1 list, including the European Union, which is exceptionally reserved on the ISO 3166-1 List, and its scope extended in August 1999 to any application needing to represent the name European Union [http:⁄⁄www.iso.org⁄iso⁄support⁄country_codes⁄iso_3166_code_lists⁄iso-3166-1_decoding_table.htm#EU].

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.

3. The list of UN member states in six official UN languages prepared by the Working Group on Country Names of the United Nations Conference on the standardization of Geographical Names

4. The 2-letter alpha-2 code of all country and territory names contained on the ISO 3166-1 list, including all reserved and unassigned codes

This comprehensive list of names will be ineligible for registration. Only in consultation with the GAC and ICANN would Donuts develop a proposal for release of these reserved names, and seek approval accordingly. Donuts understands governmental processes require time-consuming, multi-department consultations. Accordingly, we will apportion more than adequate time for the GAC and its members to review any proposal we provide.

Donuts recognizes the potential use of country and territory names at the third level. We will address and mitigate attempted third-level use of geographic names as part of our operations.

Donuts' list of geographic names will be transmitted to Registrars as part of the onboarding process and will also be made available to the public via the TLD website. Changes to the list are anticipated to be rare; however, Donuts will regularly review and revise the list as changes are made by government authorities.

For purposes of clarity the following will occur for a domain that is reserved by the registry:
1. An availability check for a domain in the reserved list will result in a "not available" status. The reason given will indicate that the domain is reserved.
2. An attempt to register a domain name in the reserved list will result in an error.
3. An EPP info request will result in an error indicating the domain name was not found.
4. Queries for a reserved name in the WHOIS system will display information indicating the reserved status and indicate it is not registered nor is available for registration.
5. Reserved names will not be published or used in the zone in any way.
6. Queries for a reserved name in the DNS will result in an NXDOMAIN response.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

Q23 CHAR: 22971

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

The following response describes our registry services, as implemented by Donuts and our partners. Such partners include Demand Media Europe Limited (DMEL) for back-end registry services; AusRegistry Pty Ltd. (ARI) for Domain Name System (DNS) services and Domain Name Service Security Extensions (DNSSEC); an independent consultant for abuse mitigation and prevention consultation; Equinix and SuperNap for datacenter facilities and infrastructure; and Iron Mountain Intellectual Property Management, Inc. (Iron Mountain) for data escrow services. For simplicity, the term "company" and the use of the possessive pronouns "we", "us", "our", "ours", etc., all refer collectively to Donuts and our subcontracted service providers.

DMEL is a wholly-owned subsidiary of DMIH Limited, a well-capitalized Irish corporation whose ultimate parent company is Demand Media, Inc., a leading content and social media company listed on the New York Stock Exchange (ticker: DMD). DMEL is structured to operate a robust and reliable Shared Registration System by leveraging the infrastructure and expertise of DMIH and Demand Media, Inc., which includes years of experience in the operation side for domain names in both gTLDs and ccTLDs for over 10 years.

1.0. EXECUTIVE SUMMARY

We offer all of the customary services for proper operation of a gTLD registry using an approach designed to support the security and stability necessary to ensure continuous uptime and optimal registry functionality for registrants and Internet users alike.

2.0. REGISTRY SERVICES

2.1. Receipt of Data from registrars

The process of registering a domain name and the subsequent maintenance involves interactions between registrars and the registry. These interactions are facilitated by the registry through the Shared Registration System (SRS) through two interfaces:

- EPP: A standards-based XML protocol over a secure network channel.
- Web: A web based interface that exposes all of the same functionality as EPP yet accessible through a web browser.

Registrants wishing to register and maintain their domain name registrations must do so through an ICANN accredited registrar. The XML protocol, called the Extensible Provisioning Protocol (EPP) is the standard protocol widely used by registrars to communicate provisioning actions. Alternatively, registrars may use the web interface to create and manage registrations.

The registry is implemented as a "thick" registry meaning that domain registrations must have contact information associated with each. Contact information will be collected by registrars and associated with domain registrations.

2.1.1. SRS EPP Interface

The SRS EPP Interface is provided by a software service that provides network based connectivity. The EPP software is highly compliant with all appropriate RFCs including:

- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP
- RFC 5910 Domain Name System (DNS) Security Extensions for Extensible Provisioning Protocol (EPP)
- RFC 3915 Domain Registry Grace Period Mapping for EPP

2.1.1.1. SRS EPP Interface Security Considerations

Security precautions are put in place to ensure transactions are received only from authorized registrars in a private, secure manner. Registrars must provide the registry with narrow subnet ranges, allowing the registry to restrict network connections that originate only from these pre-arranged networks. The source IP address is verified against the authentication data received from the connection to further validate the source of the connection. Registrars may only establish a limited number of connections and the network traffic is rate limited to ensure that all registrars receive the same quality of service. Network connections to the EPP server must be secured with TLS. The revocation status and validity of the certificate are checked.

Successful negotiation of a TLS session begins the process of authentication using the protocol elements of EPP. Registrars are not permitted to continue without a successful EPP session establishment. The EPP server validates the credential information passed by the registrar along with validation of:

- Certificate revocation status
- Certificate chain
- Certificate Common Name matches the Common Name the registry has listed for the source IP address
- User name and password are correct and match those listed for the source IP address

In the event a registrar creates a level of activity that threatens the service quality of other registrars, the service has the ability to rate limit individual registrars.

2.1.1.2. SRS EPP Interface Stability Considerations

To ensure the stability of the EPP Interface software, strict change controls and access controls are in place. Changes to the software must be approved by management and go through a rigorous testing and staged deployment procedure.

Additional stability is achieved by carefully regulating the available computing resources. A policy of conservative usage thresholds leaves an equitable amount of computing resources available to handle spikes and service management.

2.1.2. SRS Web Interface

The SRS web interface is an alternative way to access EPP functionality using a web interface, providing the features necessary for effective operations of the registry. This interface uses the HTTPS protocol for secure web communication. Because users can be located worldwide, as with the EPP interface, the web interface is available to all registrars over multiple network paths.
Additional functionality is available to registrars to assist them in managing their

account. For instance, registrars are able to view their account balance in near real time as well as the status of the registry services. In addition, notifications that are sent out in email are available for viewing.

2.1.2.1. Web Interface Security Considerations

Only registrars are authorized to use the SRS web interface, and therefore the web interface has several security measures to prevent abuse. The web interface requires an encrypted network channel using the HTTPS protocol. Attempts to access the interface through a clear channel are redirected to the encrypted channel.

The web interface restricts access by requiring each user to present authentication credentials before proceeding. In addition to the typical user name and password combinations, the web interface also requires the user to possess a hardware security key as a second factor of authentication.

Registrars are provided a tool to create and manage users that are associated with their account. With these tools, they can set access and authorization levels for their staff.

2.1.2.2. Web Interface Stability Considerations

Both the EPP interface and web interface use a common service provider to perform the work required to fulfill their requests. This provides consistency across both interfaces and ensures all policies and security rules are applied.

The software providing services for both interfaces executes on a farm of servers, distributing the load more evenly ensuring stability is maintained.

2.2. Dissemination of TLD Zone Files

2.2.1. Communication of Status Information of TLD Zone Servers to Registrars

The status of TLD zone servers and their ability to reflect changes in the SRS is of great importance to registrars and Internet users alike. We ensure that any change from normal operations is communicated to the relevant stakeholders as soon as is appropriate. Such communication might be prior to the status change, during the status change and⁄or after the status change (and subsequent reversion to normal) — as appropriate to the party being informed and the circumstance of the status change.

Normal operations are:

- DNS servers respond within SLAs for DNS resolution.
- Changes in the SRS are reflected in the zone file according to the DNS update time SLA.

The SLAs are those from Specification 10 of the Registry Agreement.

A deviation from normal operations, whether it is registry wide or restricted to a single DNS node, will result in the appropriate status communication being sent.

2.2.2. Communication Policy

We maintain close communication with registrars regarding the performance and consistency of the TLD zone servers.

A contact database containing relevant contact information for each registrar is maintained. In many cases, this includes multiple forms of contact, including email, phone and physical mailing address. Additionally, up-to-date status information of the TLD zone servers is provided within the SRS Web Interface.

Communication using the registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is required within a short timeframe, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication.

That being said, the TLD zone server infrastructure has been designed in such a way that we expect no downtime. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

2.2.3. Security and Stability Considerations

We restrict zone server status communication to registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, we ensure registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

2.3. Zone File Access Provider Integration

Individuals or organizations that wish to have a copy of the full zone file can do so using the Zone Data Access service. This process is still evolving; however the basic requirements are unlikely to change. All registries will publish the zone file in a common format accessible via secure FTP at an agreed URL.

DMEL will fully comply with the processes and procedures dictated by the Centralized Zone Data Access Provider (CZDA Provider or what it evolves into) for adding and removing Zone File access consumers from its authentication systems. This includes:

- Zone file format and location.
- Availability of the zone file access host via FTP.
- Logging of requests to the service (including the IP address, time, user and activity log).
- Access frequency.

2.4. Zone File Update

To ensure changes within the SRS are reflected in the zone file rapidly and securely, we update the zone file on the TLD zone servers following a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers - which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative primary server for the zone, but remain inaccessible to systems outside our network. The primary servers notify the designated secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes.

The mechanisms for ensuring consistency within and between updates are fully implemented in our TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions.

2.5. Operation of Zone Servers

ARI maintains TLD zone servers which act as the authoritative servers to which the TLD is delegated.

2.5.1. Security and Operational Considerations of Zone Server Operations

The potential risks associated with operating TLD zone servers are recognized by us such that we will perform the steps required to protect the integrity and consistency of the information they provide, as well as to protect the availability and accessibility of those servers to hosts on the Internet. The TLD zone servers comply with all relevant RFCs for DNS and DNSSEC, as well as BCPs for the operation and hosting of DNS servers. The TLD zone servers will be updated to support any relevant new enhancements or improvements adopted by the IETF.

The DNS servers are geographically dispersed across multiple secure data centers in strategic locations around the world. By combining multi-homed servers and geographic diversity, ARI's zone servers remain impervious to site level, supplier level or geographic level operational disruption.

The TLD zone servers are protected from accessibility loss by malicious intent or misadventure, via the provision of significant over-capacity of resources and access paths. Multiple independent network paths are provided to each TLD zone server and the query servicing capacity of the network exceeds the extremely conservatively anticipated peak load requirements by at least 10 times, to prevent loss of service should query loads significantly increase.

As well as the authentication, authorization and consistency checks carried out by the registrar access systems and DNS update mechanisms, ARI reduces the scope for alteration of DNS data by following strict DNS operational practices:

- TLD zone servers are not shared with other services.
- The primary authoritative TLD zone server is inaccessible outside ARI's network.
- TLD zone servers only serve authoritative information.
- The TLD zone is signed with DNSSEC and a DNSSEC Practice⁄Policy Statement published.

2.6. Dissemination of Domain Registration Information

Domain name registration information is required for a variety of purposes. Our registry provides this information through the required WHOIS service through a standard text based network protocol on port 43. Whois also is provided on the registry's web site using a standard web interface. Both interfaces are publically available at no cost to the user and are reachable worldwide.

The information displayed by the Whois service consists not only of the domain name but also of relevant contact information associated with the domain. It also identifies nameserver delegation and the registrar of record. This service is available to any Internet user, and use of it does not require prior authorization or permission.

2.6.1. Whois Port 43 Interface

The Whois port 43 interface consists of a standard Transmission Control Protocol (TCP) server that answers requests for information over port 43 in compliance with

IETF RFC 3912. For each query, the TCP server accepts the connection over port 43 and then waits for a set time for the query to be sent. This communication occurs via clear, unencrypted ASCII text. If a properly formatted and valid query is received, the registry database is queried for the registration data. If registration data exists, it is returned to the service where it is then formatted and delivered to the requesting client. Each query connection is short-lived. Once the output is transmitted, the server closes the connection.

2.6.2. Whois Web Interface

The Whois web interface also uses clear, unencrypted text. The web interface is in an HTML format suitable for web browsers. This interface is also available over an encrypted channel on port 43 using the HTTPS protocol.

2.6.3. Security and Stability Considerations

Abuse of the Whois system through data mining is a concern as it can impact system performance and reduce the quality of service to legitimate users. The Whois system mitigates this type of abuse by detecting and limiting bulk query access from single sources. It does this in two ways: 1) by rate limiting queries by non-authorized parties; and 2) by ensuring all queries result in responses that do not include data sets representing significant portions of the registration database.
In addition, the Whois web interface adds a simple challenge-response CAPCHA that requires a user to type in the characters displayed in image format.
Both systems have blacklist functionality to provide a complete block to individual IPs or IP ranges.

2.7. Internationalized Domain Names (IDNs)

An Internationalized Domain Name (IDN) contains at least one label that is displayed in a specific language script in IDN aware software. We will offer registration of second level IDN labels at launch,
IDNs are published into the TLD zone. The SRS EPP and Web Interfaces also support IDNs.
The IDN implementation is fully compliant with the IDNA 2008 suite of standards (RFC 5890, 5891, 5892 and 5893) as well as the ICANN Guidelines for the Implementation of IDN Version 3.0 ‹http:⁄⁄www.icann.org⁄en⁄resources⁄idn⁄implementation-guidelines› .
To ensure stability and security, we have adopted a conservative approach in our IDN registration policies, as well as technical implementation.

All IDN registrations must be requested using the A-label form, and accompanied by an RFC 5646 language tag identifying the corresponding language table published by the registry. The candidate A-label is processed according to the registration protocol as specified in Section 4 of RFC 5891, with full U-label validation. Specifically, the “Registry Restrictions” steps specified in Section 4.3 of RFC 5891 are implemented by validating the U-label against the identified language table to ensure that the set of characters in the U-label is a proper subset of the character repertoire listed in the language table.

2.7.1. IDN Stability Considerations

To avoid the intentional or accidental registration of visually similar characters, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.
Domains registered within a particular language are restricted to only the characters of that language. This avoids the use of visually similar characters within one language which mimic the appearance of a label within another language, regardless of

whether that label is already within the DNS or not.
Child domains are restricted to a specific language and registrations are prevented in one language being confused with a registration in another language; for example Cyrillic a (U+0430) and Latin a (U+0061).

2.8. DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an Internet user (normally the resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.
This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect Internet users. DNSSEC allows a domain owner to sign their domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

Registries, as the operators of the parent domain for registrants, must publish the DNSSEC material received from registrants, so that Internet users can trust the material they receive from the domain owner. This is commonly referred to as a "chain of trust." Internet users trust the root (operated by IANA), which publishes the registries' DNSSEC material, therefore registries inherit this trust. Domain owners within the TLD subsequently inherit trust from the parent domain when the registry publishes their DNSSEC material.

In accordance with new gTLD requirements, the TLD zone will be DNSSEC signed and the receipt of DNSSEC material from registrars for child domains is supported in all provisioning systems.

2.8.1. Stability and Operational Considerations for DNSSEC

2.8.1.1. DNSSEC Practice Statement

ARI's DNSSEC Practice Statement is included in our response to Question 43. The DPS following the guidelines set out in the draft IETF DNSOP DNSSEC DPS Framework document.

2.8.1.2. Resolution Stability

DNSSEC is considered to have made the DNS more trustworthy; however some transitional considerations need to be taken into account. DNSSEC increases the size and complexity of DNS responses. ARI ensures the TLD zone servers are accessible and offer consistent responses over UDP and TCP.

The increased UDP and TCP traffic which results from DNSSEC is accounted for in both network path access and TLD zone server capacity. ARI will ensure that capacity planning appropriately accommodates the expected increase in traffic over time.

ARI complies with all relevant RFCs and best practice guides in operating a DNSSEC-signed TLD. This includes conforming to algorithm updates as appropriate. To ensure Key Signing Key Rollover procedures for child domains are predictable, DS records will be published as soon as they are received via either the EPP server or SRS Web Interface. This allows child domain operators to rollover their keys with the assurance that their timeframes for both old and new keys are reliable.

3.0. APPROACH TO SECURITY AND STABILITY

Stability and security of the Internet is an important consideration for the registry system. To ensure that the registry services are reliably secured and remain stable under all conditions, DMEL takes a conservative approach with the operation and architecture of the registry system.

By architecting all registry services to use the least privileged access to systems and data, risk is significantly reduced for other systems and the registry services as a whole should any one service become compromised. By continuing that principal through to our procedures and processes, we ensure that only access that is necessary to perform tasks is given. ARI has a comprehensive approach to security modeled of the ISO27001 series of standards and explored further in the relevant questions of this response.

By ensuring all our services adhering to all relevant standards, DMEL ensures that entities which interact with the registry services do so in a predictable and consistent manner. When variations or enhancements to services are made, they are also aligned with the appropriate interoperability standards.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24 CHAR: 19964

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

1.0. INTRODUCTION

Our Shared Registration System (SRS) complies fully with Specification 6, Section 1.2 and the SLA Matrix provided with Specification 10 in ICANN’s Registry Agreement and is in line with the projections outlined in our responses to Questions 31 and 46. The services provided by the SRS are critical to the proper functioning of a TLD registry.

We will adhere to these commitments by operating a robust and reliable SRS founded on best practices and experience in the domain name industry.

2.0. TECHNICAL OVERVIEW

A TLD operator must ensure registry services are available at all times for both registrants and the Internet community as a whole. To meet this goal, our SRS was specifically engineered to provide the finest levels of service derived from a long pedigree of excellence and experience in the domain name industry. This pedigree of excellence includes a long history of technical excellence providing long running, highly available and high-performing services that help thousands of companies derive their livelihoods.

Our SRS services will give registrars standardized access points to provision and manage domain name registration data. We will provide registrars with two interfaces: an EPP protocol over TCP⁄IP and a web site accessible from any web browser (note: throughout this document, references to the SRS are inclusive of both these interfaces).

Initial registration periods will comply with Specification 6 and will be in one (1) year increments up to a maximum of ten (10) years. Registration terms will not be allowed to exceed ten (10) years. In addition, renewal periods also will be in one-year increments and renewal periods will only allow an extension of the registration period of up to ten years from the time of renewal.

The performance of the SRS is critical for the proper functioning of a TLD. Poor performance of the registration systems can adversely impact registrar systems that depend on its responsiveness. Our SRS is committed to exceeding the performance specifications described in Specification 10 in all cases. To ensure that we are well within specifications for performance, we will test our system on a regular basis during development to ensure that changes have not impacted performance in a material way. In addition, we will monitor production systems to ensure compliance. If internal thresholds are exceeded, the issue will be escalated, analyzed and addressed.

Our SRS will offer registry services that support Internationalized Domain Names (IDNs). Registrations can be made through both the EPP and web interfaces.

3.0. ROBUST AND RELIABLE ARCHITECTURE
To ensure quality of design, the SRS software was designed and written by seasoned and experienced software developers. This team designed the SRS using modern software architecture principles geared toward ensuring flexibility in its design not only to meet business needs but also to make it easy to understand, maintain and test.

A classic 3-tier design was used for the architecture of the system. 3-tier is a well-proven architecture that brings flexibility to the system by abstracting the application layer from the protocol layer. The data tier is isolated and only accessible by the services tier. 3-tier adds an additional layer of security by minimizing access to the data tier through possible exploits of the protocol layer.

The protocol and services layers are fully redundant. A minimum of three physical servers is in place in both the protocol and services layers. Communications are balanced across the servers. Load balancing is accomplished with a redundant load balancer pair.

4.0. SOFTWARE QUALITY

The software for the SRS, as well as other registry systems, was developed using an approach that ensures that every line of source code is peer reviewed and source code is not checked into the source code repository without the accompanying automated tests that exercise the new functionality. The development team responsible for building the SRS and other registry software applies continuous integration practices to all software projects; all developers work on an up-to-date code base and are required to synchronize their code base with the master code base and resolve any incompatibilities before checking in. Every source code check-in triggers an automated build and test process to ensure a minimum level of quality. Each day an automated “daily build” is created, automatically deployed to servers and a fully-automated test suite run against it. Any failures are automatically assigned to developers to resolve in the morning when they arrive.

When extensive test passes are in order for release candidates, these developers use a test harness designed to run usability scenarios that exercise the full gamut of use cases, including accelerated full registration life cycles. These scenarios can be entered into the system using various distributions of activity. For instance, the test harness can be run to stress the system by changing the distribution of scenarios or to stress the system by exaggerating particular scenarios to simulate land rushes or, for long running duration scenarios, a more common day-to-day business distribution.

5.0. SOFTWARE COMPLIANCE

The EPP interface to our SRS is compliant with current RFCs relating to EPP protocols and best practices. This includes RFCs 5910, 5730, 5731, 5732, 5733 and 5734. Since we are also supporting Registry Grace Period functionality, we are also compliant with RFC 3915. Details of our compliance with these specifications are provided in our response to Question 25. We are also committed to maintaining compliance with future RFC revisions as they apply as documented in Section 1.2 of Specification 6 of the new gTLD Agreement.

We strive to be forward-thinking and will support the emerging standards of both IPv6 and DNSSEC on our SRS platform. The SRS was designed and has been tested to accept IPv6 format addresses for nameserver glue records and provision them to the gTLD zone. In addition, key registry services will be accessible over both IPv4 and IPv6. These include both the SRS EPP and SRS web-based interfaces, both port 43 and web-based WHOIS interfaces and DNS, among others. For details regarding our IPv6 reachability plans, please refer to our response to Question 36.

DNSSEC services are provided, and we will comply with Specification 6. Additionally, our DNSSEC implementation complies with RFCs 4033, 4034, 4035, and 4509; and we commit to complying with the successors of these RFCs and following the best practices described in RFC 4641. Additional compliance and commitment details on our DNSSEC services can be found in our response to Question 43.

6.0. DATABASE OPERATIONS

The database for our gTLD is Microsoft SQL Server 2008 R2. It is an industry-leading database engine used by companies requiring the highest level of security, reliability and trust. Case studies highlighting SQL Server’s reliability and use indicate its successful application in many industries, including major financial institutions such as Visa, Union Bank of Israel, KeyBank, TBC Bank, Paymark, Coca-Cola, Washington State voter registration and many others. In addition, Microsoft SQL Server provides a number of features that ease the management and maintenance of the system. Additional details about our database system can be found in our response to Question 33.

Our SRS architecture ensures security, consistency and quality in a number of ways. To prevent eavesdropping, the services tier communicates with the database over a secure channel. The SRS is architected to ensure all data written to the database is atomic. By convention, leave all matters of atomicity are left to the database. This ensures consistency of the data and reduces the chance of error. So that we can examine data versions at any point in time, all changes to the database are written to an audit database. The audit data contains all previous and new values and the date⁄time of the change. The audit data is saved as part of each atomic transaction to ensure consistency.

To minimize the chance of data loss due to a disk failure, the database uses an array of redundant disks for storage. In addition, maintain an exact duplicate of the primary site is maintained in a secondary datacenter. All hardware is fully duplicated and set up to take over operations at any time. All database operations are replicated to the secondary datacenter via synchronous replication. The secondary datacenter always maintains an exact copy of our live data as the transactions occur.

7.0. REDUNDANT HARDWARE

The SRS is composed of several pieces of hardware that are critical to its proper functioning, reliability and scale. At least two of each hardware component comprises the SRS, making the service fully redundant. Any component can fail, and the system is designed to use the facility of its pair. The EPP interface to the SRS will operate with more than two servers to provide the capacity required to meet our projected scale as described in Question 46: Projections Template.

8.0. HORIZONTALLY SCALABLE

The SRS is designed to scale horizontally. That means that, as the needs of the registry grow, additional servers can be easily added to handle additional loads.

The database is a clustered 2-node pair configured for both redundancy and performance. Both nodes participate in serving the needs of the SRS. A single node can easily handle the transactional load of the SRS should one node fail. In addition, there is an identical 2-node cluster in our backup datacenter. All data from the primary database is continuously replicated to the backup datacenter.

Not only is the registry database storage medium specified to provide the excess of capacity necessary to allow for significant growth, it is also configured to use techniques, such as data sharing, to achieve horizontal scale by distributing logical groups of data across additional hardware. For further detail on the scalability of our SRS, please refer to our response to Question 31.

9.0. REDUNDANT HOT FAILOVER SITE

We understand the need for maximizing uptime. As such, our plan includes maintaining at all times a warm failover site in a separate datacenter for the SRS and other key registry services. Our planned failover site contains an exact replica of the hardware and software configuration contained in the primary site. Registration data will be replicated to the failover site continuously over a secure connection to keep the failover site in sync.

Failing over an SRS is not a trivial task. In contrast, web site failover can be as simple as changing a DNS entry. Failing over the SRS, and in particular the EPP interface, requires careful planning and consideration as well as training and a well-documented procedure. Details of our failover procedures as well as our testing plans are detailed in our response to Question 41.

10.0. SECURE ACCESS

To ensure security, access to the EPP interface by registrars is restricted by IP⁄subnet. Access Control Lists (ACLs) are entered into our routers to allow access only from a restricted, contiguous subnet from registrars. Secure and private communication over mutually authenticated TLS is required. Authentication credentials and certificate data are exchanged in an out-of-band mechanism. Connections made to the EPP interface that successfully establish an EPP session are subject to server policies that dictate connection maximum lifetime and minimal activity to maintain the session.

To ensure fair and equal access for all registrars, as well as maintain a high level of service, we will use traffic shaping hardware to ensure all registrars receive an equal number of resources from the system.

To further ensure security, access to the SRS web interface is over the public Internet via an encrypted HTTPS channel. Each registrar will be issued master credentials for accessing the web interface. Each registrar also will be required to use 2-factor authentication when logging in. We will issue a set of Yubikey (http:⁄⁄yubico.com) 2-factor, one-time password USB keys for authenticating with the web site. When the SRS web interface receives the credentials plus the one-time password from the Yubikey, it communicates with a RADIUS authentication server to check the credentials.

11.0. OPERATING A ROBUST AND RELIABLE SRS

11.1. AUTOMATED DEPLOYMENT

To minimize human error during a deployment, we use a fully-automated package and deployment system. This system ensures that all dependencies, configuration changes and database components are included every time. To ensure the package is appropriate for the system, the system also verifies the version of system we are upgrading.

11.2. CHANGE MANAGEMENT

We use a change management system for changes and deployments to critical systems. Because the SRS is considered a critical system, it is also subject to all change management procedures. The change management system covers all software development changes, operating system and networking hardware changes and patching. Before implementation, all change orders entered into the system must be reviewed with careful scrutiny and approved by appropriate management. New documentation and procedures are written; and customer service, operations, and monitoring staff are trained on any new functionality added that may impact their areas.

11.3. PATCH MANAGEMENT

Upon release, all operating system security patches are tested in the staging environment against the production code base. Once approved, patches are rolled out to one node of each farm. An appropriate amount of additional time is given for further validation of the patch, depending on the severity of the change. This helps minimize any downtime (and the subsequent roll back) caused by a patch of poor quality. Once validated, the patch is deployed on the remaining servers.

11.4. REGULAR BACKUPS

To ensure that a safe copy of all data is on hand in case of catastrophic failure of all database storage systems, backups of the main database are performed regularly. We perform full backups on both a weekly and monthly basis. We augment these full backups with differential backups performed daily. The backup process is monitored and any failure is immediately escalated to the systems engineering team. Additional details on our backup strategy and procedures can be found in our response to Question 37.

11.5. DATA ESCROW

Data escrow is a critical registry function. Escrowing our data on a regular basis ensures that a safe, restorable copy of the registration data is available should all other attempts to restore our data fail. Our escrow process is performed in accordance with Specification 2. Additional details on our data escrow procedures can be found in our response to Question 38.

11.6. REGULAR TRAINING

Ongoing security awareness training is critical to ensuring users are aware of security threats and concerns. To sustain this awareness, we have training programs in place designed to ensure corporate security policies pertaining to registry and other operations are understood by all personnel. All employees must pass a proficiency exam and sign the Information Security Policy as part of their employment. Further detail on our security awareness training can be found in our response to Question 30a.

We conduct failover training regularly to ensure all required personnel are up-to-date on failover process and have the regular practice needed to ensure successful failover should it be necessary. We also use failover training to validate current policies and procedures. For additional details on our failover training, please refer to our response to Question 41.

11.7. ACCESS CONTROL

User authentication is required to access any network or system resource. User accounts are granted the minimum access necessary. Access to production resources is restricted to key IT personnel. Physical access to production resources is extremely limited and given only as needed to IT-approved personnel. For further details on our access control policies, please refer to our response to Question 30a.

11.8. 24⁄7 MONITORING AND REGISTRAR TECHNICAL SUPPORT

We employ a full-time staff trained specifically on monitoring and supporting the services we provide. This staff is equipped with documentation outlining our processes for providing first-tier analysis, issue troubleshooting, and incident handling. This team is also equipped with specialty tools developed specifically to safely aid in diagnostics. On-call staff second-tier support is available to assist when necessary. To optimize the service we provide, we conduct ongoing training in both basic and more advanced customer support and conduct additional training, as needed, when new system or tool features are introduced or solutions to common issues are developed.

12.0. SRS INFRASTRUCTURE

As shown in Attachment A, Figure 1, our SRS infrastructure consists of two identically provisioned and configured datacenters with each served by multiple bandwidth providers.

For clarity in Figure 1, connecting lines through the load balancing devices between the Protocol Layer and the Services Layer are omitted. All hardware connecting to the Services Layer goes through a load-balancing device. This device distributes the load across the multiple machines providing the services. This detail is illustrated more clearly in subsequent diagrams in Attachment A.

13.0 RESOURCING PLAN

Resources for the continued development and maintenance of the SRS and ancillary services have been carefully considered. We have a significant portion of the required personnel on hand and plan to hire additional technical resources, as indicated below. Resources on hand are existing full time employees whose primary responsibility is the SRS.

For descriptions of the following teams, please refer to the resourcing section of our response to Question 31, Technical Review of Proposed Registry. Current and planned allocations are below.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, two, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, 2 Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

25. Extensible Provisioning Protocol (EPP)

Q25 CHAR: 20820

TLD Applicant is applying to become an ICANN accredited Top Level Domain (TLD) registry. TLD Applicant meets the operational, technical, and financial capability requirements to pursue, secure and operate the TLD registry. The responses to technical capability questions were prepared to demonstrate, with confidence, that the technical capabilities of TLD Applicant meet and substantially exceed the requirements proposed by ICANN.

1.0. INTRODUCTION

Our SRS EPP interface is a proprietary network service compliant with RFC 3735 and RFCs 5730-4. The EPP interface gives registrars a standardized programmatic access point to provision and manage domain name registrations.

2.0. IMPLEMENTATION EXPERIENCE

The SRS implementation for our gTLD leverages extensive experience implementing long-running, highly available network services accessible. Our EPP interface was written by highly experienced engineers focused on meeting strict requirements developed to ensure quality of service and uptime. The development staff has extensive experience in the domain name industry.

3.0. TRANSPORT

The EPP core specification for transport does not specify that a specific transport method be used and is, thus, flexible enough for use over a variety of transport methods. However, EPP is most commonly used over TCP⁄IP and secured with a Transport Layer Security (TLS) layer for domain registration purposes. Our EPP interface uses the industry standard TCP with TLS.

4.0. REGISTRARS’ EXPERIENCE

Registrars will find our EPP interface familiar and seamless. As part of the account creation process, a registrar provides us with information we use to authenticate them. The registrar provides us with two subnets indicating the connection’s origination. In addition, the registrar provides us with the Common Name specified in the certificate used to identify and validate the connection.

Also, as part of the account creation process, we provide the registrar with authentication credentials. These credentials consist of a client identifier and an initial password and are provided in an out-of-band, secure manner. These credentials are used to authenticate the registrar when starting an EPP session.

Prior to getting access to the production interfaces, registrars have access to an Operational Test and Evaluation (OT&E) environment. This environment is an isolated area that allows registrars to develop and test against registry systems without any impact to production. The OT&E environment also provides registrars the opportunity to test implementation of custom extensions we may require.

Once a registrar has completed testing and is prepared to go live, the registrar is provided a Scripted Server Environment. This environment contains an EPP interface and database pre-populated with known data. To verify that the registrar’s implementations are correct and minimally suitable for the production environment, the registrar is required to run through a series of exercises. Only after successful performance of these exercises is a registrar allowed access to production services.

5.0. SESSIONS

The only connections that are allowed are those from subnets previously communicated during account set up. The registrar originates the connection to the SRS and must do so securely using a Transport Layer Security (TLS) encrypted channel over TCP⁄IP using the IANA assigned standard port of 700.

The TLS protocol establishes an encrypted channel and confirms the identity of each machine to its counterpart. During TLS negotiation, certificates are exchanged to mutually verify identities. Because mutual authentication is required, the registrar certificate must be sent during the negotiation. If it is not sent, the connection is terminated and the event logged.

The SRS first examines the Common Name (CN). The SRS then compares the Common Name to the one provided by the registrar during account set up. The SRS then validates the certificate by following the signature chain, ensures that the chain is complete, and terminates against our store of root Certificate Authorities (CA). The SRS also verifies the revocation status with the root CA. If these fail, the connection is terminated and the event logged.

Upon successful completion of the TLS handshake and the subsequent client validation, the SRS automatically sends the EPP greeting. Then the registrar initiates a new session by sending the login command with their authentication credentials. The SRS passes the credentials to the database for validation over an encrypted channel. Policy limits the number of failed login attempts. If the registrar exceeds the maximum number of attempts, the connection to the server is closed. If authentication was successful, the EPP session is allowed to proceed and a response is returned indicating that the command was successful.

An established session can only be maintained for a finite period. EPP server policy specifies the timeout and maximum lifetime of a connection. The policy requires the registrar to send a protocol command within a given timeout period. The maximum lifetime policy for our registry restricts the connection to a finite overall timespan. If a command is not received within the timeout period or the connection lifetime is exceeded, the connection is terminated and must be reestablished. Connection lifecycle details are explained in detail in our Registrar Manual.

The EPP interface allows pipelining of commands. For consistency, however, the server only processes one command at a time per session and does not examine the next command until a response to the previous command is sent. It is the registrar’s responsibility to track both the commands and their responses.

6.0. EPP SERVICE SCALE

Our EPP service is horizontally scalable. Its design allows us to add commodity-grade hardware at any time to increase our capacity. The design employs a 3-tier architecture which consists of protocol, services and data tiers. Servers for the protocol tier handle the loads of SSL negotiation and protocol validation and parsing. These loads are distributed across a farm of numerous servers balanced by load-balancing devices. The protocol tier connects to the services tier through load-balancing devices.

The services tier consists of a farm of servers divided logically based on the services provided. Each service category has two or more servers. The services tier is responsible for registry policy enforcement, registration lifecycle and provisioning, among other services. The services tier connects to the data tier which consists of Microsoft SQL Server databases for storage.

The data tier is a robust SQL Server installation that consists of a 2-node cluster in an active⁄active configuration. Each node is designed to handle the entire load of the registry should the alternate node go offline.

Additional details on scale and our plans to service the load we anticipate are described in detail on questions 24: SRS Performance and 32: Architecture.

7.0. COMPLIANCE WITH CORE AND EPP EXTENSION RFCs

The EPP interface is highly compliant with the following RFCs:

- RFC 5730 Extensible Provisioning Protocol
- RFC 5731 EPP Domain Name Mapping
- RFC 5732 EPP Host Mapping
- RFC 5733 EPP Contact Mapping
- RFC 5734 EPP Transport over TCP
- RFC 3915 Domain Registry Grace Period Mapping
- RFC 5910 Domain Name System (DNS) Security Extensions Mapping

The implementation is fully compliant with all points in each RFC. Where an RFC specifies optional details or service policy, they are explained below.

7.1. RFC 5730 EXTENSIBLE PROVISIONING PROTOCOL

Section 2.1 Transport Mapping Considerations - ack.
Transmission Control Protocol (TCP) in compliance with RFC 5734 with TLS.

Section 2.4 Greeting Format – compliant
The SRS implementation responds to a successful connection and subsequent TLS handshake with the EPP Greeting. The EPP Greeting is also transmitted in response to a ⟨hello⁄⟩ command. The server includes the EPP versions supported which at this time is only 1.0. The Greeting contains namespace URIs as ⟨objURI⁄⟩ elements representing the objects the server manages.

The Greeting contains a ⟨svcExtension⟩ element with one ⟨extURI⟩ element for each extension namespace URI implemented by the SRS.

Section 2.7 Extension Framework – compliant
Each mapping and extension, if offered, will comply with RFC 3735 Guidelines for Extending EPP.

Section 2.9 Protocol Commands – compliant

Login command’s optional ⟨options⟩ element is currently ignored. The ⟨version⟩ is verified and 1.0 is currently the only acceptable response. The ⟨lang⟩ element is also ignored because we currently only support English (en). This server policy is reflected in the greeting.

The client mentions ⟨objURI⟩ elements that contain namespace URIs representing objects to be managed during the session inside ⟨svcs⟩ element of Login request. Requests with unknown ⟨objURI⟩ values are rejected with error information in the response. A ⟨logout⟩ command ends the client session.

Section 4 Formal syntax - compliant
All commands and responses are validated against applicable XML schema before acting on the command or sending the response to the client respectively. XML schema validation is performed against base schema (epp-1.0), common elements schema (eppcom-1.0) and object-specific schema.

Section 5 Internationalization Considerations - compliant
EPP XML recognizes both UTF-8 and UTF-16. All date-time values are presented in Universal Coordinated Time using Gregorian calendar.

7.2. RFC 5731 EPP DOMAIN NAME MAPPING

Section 2.1 Domain and Host names - compliant
The domain and host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

Section 2.2 Contact and Client Identifiers - compliant
All EPP contacts are identified by a server-unique identifier. Contact identifiers conform to “clIDType” syntax described in RFC 5730.

Section 2.3 Status Values - compliant
A domain object always has at least one associated status value. Status value can only be set by the sponsoring client or the registry server where it resides. Status values set by server cannot be altered by client. Certain combinations of statuses are not permitted as described by RFC.

Section 2.4 Dates and Times - compliant
Date and time attribute values are represented in Universal Coordinated Time (UTC) using Gregorian calendar, in conformance with XML schema.

Section 2.5 Validity Periods - compliant
Our SRS implementation supports validity periods in unit year (“y”). The default period is 1y.

Section 3.1.1 EPP 〈check〉 Command - compliant
A maximum of 5 domains can be checked in a single command request as defined by server policy.

Section 3.1.2 EPP 〈info〉 Command - compliant
EPP 〈info〉 command is used to retrieve information associated with a domain object. If the querying Registrar is not the sponsoring registrar and the registrar does not provide valid authorization information, the server does not send any domain elements in response per server policy.

Section 3.1.3 EPP 〈transfer〉 Query Command - compliant
EPP 〈transfer〉 command provides a query operation that allows a client to determine the real-time status of pending and completed transfer requests. If the authInfo element is not provided or authorization information is invalid, the command is rejected for authorization.

Section 3.2.4 EPP 〈transfer〉 Command - compliant
All subordinate host objects to the domain are transferred along with the domain object.

7.3. RFC 5732 EPP HOST MAPPING

Section 2.1 Host Names - compliant
The host names are validated to meet conformance requirements mentioned in RFC 0952, 1123 and 3490.

Section 2.2 Contact and Client Identifiers - compliant
All EPP clients are identified by a server-unique identifier. Client identifiers conform to “clIDType” syntax described in RFC 5730.

Section 2.5 IP Addresses - compliant
The syntax for IPv4 addresses conform to RFC0791. The syntax for IPv6 addresses conform to RFC4291.

Section 3.1.1 EPP 〈check〉 Command - compliant
Maximum of five host names can be checked in a single command request set by server policy.

Section 3.1.2 EPP 〈info〉 Command - compliant
If the querying client is not a sponsoring client, the server does not send any host object elements in response and the request is rejected for authorization according to server policy.

Section 3.2.2 EPP 〈delete〉 Command - compliant
A delete is permitted only if the host is not delegated.

Section 3.2.2 EPP 〈update〉 Command - compliant
Any request to change host name of an external host that has associations with objects that are sponsored by a different client fails.

7.4. RFC 5733 EPP CONTACT MAPPING

Section 2.1 Contact and Client Identifiers - compliant
Contact identifiers conform to “clIDType” syntax described in RFC 5730.

Section 2.6 Email Addresses - compliant
Email address validation conforms to syntax defined in RFC5322.

Section 3.1.1 EPP 〈check〉 Command - compliant
Maximum of 5 contact id can be checked in a single command request.

Section 3.1.2 EPP 〈info〉 Command - compliant
If querying client is not sponsoring client, server does not send any contact object elements in response and the request is rejected for authorization.

Section 3.2.2 EPP 〈delete〉 Command - compliant
A delete is permitted only if the contact object is not associated with other known objects.

7.5. RFC 5734 EPP TRANSPORT OVER TCP

Section 2 Session Management - compliant
The SRS implementation conforms to the required flow mentioned in the RFC for initiation of a connection request by a client, to establish a TCP connection. The client has the ability to end the session by issuing an EPP 〈logout〉 command, which ends the session and closes the TCP connection. Maximum life span of an established TCP connection is defined by server policy. Any connections remaining open beyond that are terminated. Any sessions staying inactive beyond the timeout policy of the server are also terminated similarly. Policies regarding timeout and lifetime values are clearly communicated to registrars in documentation provided to them.

Section 3 Message Exchange - compliant
With the exception of EPP server greeting, EPP messages are initiated by EPP client in the form of EPP commands. Client-server interaction works as a command-response exchange where the client sends one command to the server and the server returns one response to the client in the exact order as received by the server.

Section 8 Security considerations - ack.
TLS 1.0 over TCP is used to establish secure communications from IP restricted clients. Validation of authentication credentials along with the certificate common

name, validation of revocation status and the validation of the full certificate chain are performed. The ACL only allows connections from subnets prearranged with the Registrar.

Section 9 TLS Usage Profile – ack.
The SRS uses TLS 1.0 over TCP and matches the certificate common name. The full certificate chain, revocation status and expiry date is validated. TLS is implemented for mutual client and server authentication.

8.0. EPP EXTENSIONS

8.1. STANDARDIZED EXTENSIONS

Our implementation includes extensions that are accepted standards and fully documented. These include the Registry Grace Period Mapping and DNSSEC.

8.2. COMPLIANCE WITH RFC 3735

RFC 3735 are the Guidelines for Extending the Extensible Provisioning Protocol. Any custom extension implementations follow the guidance and recommendations given in RFC 3735.

8.3. COMPLIANCE WITH DOMAIN REGISTRY GRACE PERIOD MAPPING RFC 3915

Section 1 Introduction – compliant
Our SRS implementation supports all specified grace periods particularly, add grace period, auto-renew grace period, renew grace period, and transfer grace period.

Section 3.2 Registration Data and Supporting Information – compliant
Our SRS implementation supports free text and XML markup in the restore report.

Section 3.4 Client Statements – compliant
Client can use free text or XML markup to make 2 statements regarding data included in a restore report.

Section 5 Formal syntax - compliant
All commands and responses for this extension are validated against applicable XML schema before acting on the command or sending the response to the client respectively. XML schema validation is performed against RGP specific schema (rgp-1.0).

8.4. COMPLIANCE WITH DOMAIN NAME SYSTEM (DNS) SECURITY EXTENSIONS MAPPING RFC 5910

RFC 5910 describes an Extensible Provisioning Protocol (EPP) extension mapping for the provisioning and management of Domain Name System Security Extensions (DNSSEC) for domain names stored in a shared central repository. Our SRS and DNS implementation supports DNSSEC.

The information exchanged via this mapping is extracted from the repository and used to publish DNSSEC Delegate Signer (DS) resource records (RR) as described in RFC 4034.

Section 4 DS Data Interface and Key Data Interface – compliant
Our SRS implementation supports only DS Data Interface across all commands applicable with DNSSEC extension.

Section 4.1 DS Data Interface – compliant

The client can provide key data associated with the DS information. The collected key data along with DS data is returned in an info response, but may not be used in our systems.

Section 4.2 Key Data Interface - compliant
Since our gTLD's SRS implementation does not support Key Data Interface, when a client sends a command with Key Data Interface elements, it is rejected with error code 2306.

Section 5.1.2 EPP 〈info〉 Command - compliant
This extension does not add any elements to the EPP 〈info〉 command. When an 〈info〉 command is processed successfully, the EPP 〈resData〉 contains child elements for EPP domain mapping. In addition, it contains a child 〈secDNS:infData〉 element that identifies extension namespace if the domain object has data associated with this extension. It is conditionally based on whether or the client added the 〈extURI〉 element for this extension in the 〈login〉 command. Multiple DS data elements are supported.

Section 5.2.1 EPP 〈create〉 Command - compliant
The client must add an 〈extension〉 element, and the extension element MUST contain a child 〈secDNS:create〉 element if the client wants to associate data defined in this extension to the domain object. Multiple DS data elements are supported. Since the SRS implementation does not support maxSigLife, it returns a 2102 error code if the command included a value for maxSigLife.

Section 5.2.5 EPP 〈update〉 Command - compliant
Since the SRS implementation does not support the 〈secDNS:update〉 element's optional "urgent" attribute, an EPP error result code of 2102 is returned if the "urgent" attribute is specified in the command with value of Boolean true.

8.5. PROPRIETARY EXTENSION DOCUMENTATION

We are not proposing any proprietary EPP extensions for this TLD.

8.6. EPP CONSISTENT WITH THE REGISTRATION LIFECYCLE DESCRIBED IN QUESTION 27

Our EPP implementation makes no changes to the industry standard registration lifecycle and is consistent with the lifecycle described in Question 27.

9.0. RESOURCING PLAN

For descriptions of the following teams, please refer to our response to Question 31. Current and planned allocations are below.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, 2 Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, two Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

26. Whois

Q26 CHAR: 19908

1.0. INTRODUCTION

Our registry provides a publicly available Whois service for registered domain names in the top-level domain (TLD). Our planned registry also offers a searchable Whois service that includes web-based search capabilities by domain name, registrant name, postal address, contact name, registrar ID and IP addresses without an arbitrary limit. The Whois service for our gTLD also offers Boolean search capabilities, and we have initiated appropriate precautions to avoid abuse of the service. This searchable Whois service exceeds requirements and is eligible for a score of 2 by providing the following:

- Web-based search capabilities by domain name, registrant name, postal address, contact names, registrar IDs, and Internet Protocol addresses without arbitrary limit.
- Boolean search capabilities.
- Appropriate precautions to avoid abuse of this feature (e.g., limiting access to legitimate authorized users).
- Compliance with any applicable privacy laws or policies.

The Whois service for our planned TLD is available via port 43 in accordance with RFC 3912. Also, our planned registry includes a Whois web interface. Both provide free public query-based access to the elements outlined in Specification 4 of the Registry Agreement. In addition, our registry includes a searchable Whois service. This service is available to authorized entities and accessible from a web browser.

2.0. HIGH-LEVEL WHOIS SYSTEM DESCRIPTION

The Whois service for our registry provides domain registration information to the public. This information consists not only of the domain name but also of relevant contact information associated with the domain. It also identifies nameserver delegation and the registrar of record. This service is available to any Internet user, and use does not require prior authorization or permission. To maximize accessibility to the data, Whois service is provided over two mediums, as described below. Where the medium is not specified, any reference to Whois pertains to both mediums. We describe our searchable Whois solution in Section 11.0.

One medium used for our gTLD's Whois service is port 43 Whois. This consists of a standard Transmission Control Protocol (TCP) server that answers requests for information over port 43 in compliance with IETF RFC 3912. For each query, the TCP server accepts the connection over port 43 and then waits for a set time for the query to be sent. This communication occurs via clear, unencrypted text. If no query is received by the server within the allotted time or a malformed query is detected, the connection is closed. If a properly formatted and valid query is received, the registry database is queried for the registration data. If registration data exists, it is returned to the service where it is then formatted and delivered to the requesting client. Each query connection is short-lived. Once the output is transmitted, the server closes the connection.

The other medium used for Whois is via web interface using clear, unencrypted text. The web interface is in an HTML format suitable for web browsers. This interface is also available over an encrypted channel on port 443 using the HTTPS protocol.

The steps for accessing the web-based Whois will be prominently displayed on the registry home page. The web-based Whois is for interactive use by individual users while the port 43 Whois system is for automated use by computers and lookup clients.

Both Whois service offerings comply with Specification 4 of the New GTLD Agreement. Although the Whois output is free text, it follows the output format as described for domain, registrar and nameserver data in Sections 1.4, 1.5 and 1.6 of Specification 4 of the Registry Agreement.

Our gTLD's WHOIS service is mature, and its current implementation has been in continuous operation for seven years. A dedicated support staff monitors this service 24/7. To ensure high availability, multiple redundant servers are maintained to enable capacity well above normal query rates.

Most of the queries sent to the port 43 Whois service are automated. The Whois service contains mechanisms for detecting abusive activity and, if abuse is detected, reacts appropriately. This capability contributes to a high quality of service and availability for all users.

2.1. PII POLICY

The services and systems for this gTLD do not collect, process or store any personally identifiable information (PII) as defined by state disclosure and privacy laws. Registry systems collect the following Whois data types: first name, last name, address and phone numbers of all billing, administration and technical contacts. Any business conducted where confidential PII consisting of customer payment information is collected uses systems that are completely separate from registry systems and segregated at the network layer.

3.0. RELEVANT NETWORK DIAGRAM(S)

Our network diagram (Q 26 - Attachment A, Figure 1) provides a quick-reference view of the Whois system. This diagram reflects the Whois system components and compliance descriptions and explanations that follow in this section.

3.1. NARRATIVE FOR Q26 - FIGURE 1 OF 1 (SHOWN IN ATTACHMENT A)

The Whois service for our gTLD operates from two datacenters from replicated data. Network traffic is directed to either of the datacenters through a global load balancer. Traffic is directed to an appropriate server farm, depending on the service interface requested. The load balancer within the datacenter monitors the load and health of each individual server and uses this information to select an appropriate server to handle the request.

The protocol server handling the request communicates over an encrypted channel with the Whois service provider through a load-balancing device. The WHOIS service provider communicates directly with a replicated, read-only copy of the appropriate data from the registry database. The Whois service provider is passed a sanitized and verified query, such as a domain name. The database attempts to locate the appropriate records, then format and return them. Final output formatting is performed by the requesting server and the results are returned back to the original client.

4.0. INTERCONNECTIVITY WITH OTHER REGISTRY SYSTEMS

The Whois port 43 interface runs as an unattended service on servers dedicated to this task. As shown in Attachment A, Figure 1, these servers are delivered network traffic by redundant load-balancing hardware, all of which is protected by access control methods. Balancing the load across many servers helps distribute the load and allows for expansion. The system's design allows for the rapid addition of new servers, typically same-day, should load require them.

Both our port 43 Whois and our web-based Whois communicate with the Whois service provider in the middle tier. Communication to the Whois service provider is distributed by a load balancing pair. The Whois service provider calls the appropriate procedures in the database to search for the registration records.

The Whois service infrastructure operates from both datacenters, and the global load balancer distributes Whois traffic evenly across the two datacenters. If one datacenter is not responding, the service sends all traffic to the remaining datacenter. Each datacenter has sufficient capacity to handle the entire load.

To avoid placing an abnormal load on the Shared Registration System (SRS), both service installations read from replicated, read-only database instances (see Figure 1). Because each instance is maintained via replication from the primary SRS database, each replicated database contains a copy of the authoritative data. Having the Whois service receive data from this replicated database minimizes the impact of services competing for the same data and enables service redundancy. Data replication is also monitored to prevent detrimental impact on the primary SRS.

5.0. FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS

As shown in Figure 1, the system replicates WHOIS services data continuously from the authoritative database to the replicated database. This persistent connection is maintained between the databases, and each transaction is queued and published as an atomic unit. Delays, if any, in the replication of registration information are minimal, even during periods of high load. At no time will the system prioritize replication over normal operations of the SRS.

6.0. POTENTIAL FORMS OF ABUSE

Potential forms of abuse of this feature, and how they are mitigated, are outlined below. For additional information on our approach to preventing and mitigating Whois service abuse, please refer to our response to Question 28.

6.1. DATA MINING ABUSE

This type of abuse consists primarily of a user using queries to acquire all or a significant portion of the registration database.

The system mitigates this type of abuse by detecting and limiting bulk query access from single sources. It does this in two ways: 1) by rate-limiting queries by non-authorized parties; and 2) by ensuring all queries result in responses that do not include data sets representing significant portions of the registration database.

6.2. INVALID DATA INJECTION

This type of abuse is mitigated by 1) ensuring that all Whois systems are strictly read-only; and 2) ensuring that any input queries are properly sanitized to prevent data injection.

6.3. DISCLOSURE OF PRIVATE INFORMATION

The Whois system mitigates this type of abuse by ensuring all responses, while complete, only contain information appropriate to Whois output and do not contain any private or non-public information.

7.0. COMPLIANCE WITH WHOIS SPECIFICATIONS FOR DATA OBJECTS, BULK ACCESS, AND LOOKUPS

Whois specifications for data objects, bulk access, and lookups for our gTLD are fully compliant with Specifications 4 and 10 to the Registry Agreement, as explained below.

7.1. COMPLIANCE WITH SPECIFICATION 4

Compliance of Whois specifications with Specification 4 is as follows:

- Registration Data Directory Services Component: Specification 4.1 is implemented as described. Formats follow the outlined semi-free text format. Each data object is represented as a set of key⁄value pairs with lines beginning with keys followed by a colon and a space as delimiters, followed by the value. Fields relevant to RFCs 5730-4 are formatted per Section 1.7 of Specification 4.
- Searchability compliance is achieved by implementing, at a minimum, the specifications in section 1.8 of specification 4. We describe this searchability feature in Section 11.0.
- Co-operation, ICANN Access and Emergency Operator Access: Compliance with these specification components is assured.
- Bulk Registration Data Access to ICANN: Compliance with this specification component is assured.

Evidence of Whois system compliance with this specification consists of:

- Matching existing Whois output with specification output to verify that it is equivalent.

7.2. COMPLIANCE WITH SPECIFICATION 10 FOR WHOIS

Our gTLD's Whois complies fully with Specification 10. With respect to Section 4.2, the approach used ensures that Round-Trip Time (RTT) remains below five times the corresponding Service Level Requirement (SLR).

7.2.1. Emergency Thresholds

To achieve compliance with this Specification 10 component, several measures are used to ensure emergency thresholds are never reached:

1) Provide staff training as necessary on Registry Transition plan components that prevent Whois service interruption in case of emergency (see the Question 40 response for details).
2) Conduct regular failover testing for Whois services as outlined in the Question 41 response.
3) Adhere to recovery objectives for Whois as outlined in the Question 39 response.

7.2.2. Emergency Escalation

Compliance with this specification component is achieved by participation in escalation procedures as outlined in this section.

8.0. COMPLIANCE WITH RFC 3912

Whois service for our gTLD is fully compliant with RFC 3912 as follows:

- RFC 3912 Element, "A Whois server listens on TCP port 43 for requests from Whois clients": This requirement is properly implemented, as described in Section 1 above. Further, running Whois on ports other than port 43 is an option.
- RFC 3912 Element, "The Whois client makes a text request to the Whois server, then the Whois server replies with text content": The port 43 Whois service is a text-based query and response system. Thus, this requirement is also properly implemented.
- RFC 3912 Element, "All requests are terminated with ASCII CR and then ASCII LF. The response might contain more than one line of text, so the presence of ASCII CR or ASCII LF characters does not indicate the end of the response": This requirement is properly implemented for our TLD.
- RFC 3912 Element, "The Whois server closes its connection as soon as the output is finished": This requirement is properly implemented for our TLD, as described in Section 1 above.
- RFC 3912 Element, "The closed TCP connection is the indication to the client that the response has been received": This requirement is properly implemented.

9.0. RESOURCING PLAN

Resources for the continued development and maintenance of the Whois have been carefully considered. Many of the required personnel are already in place. Where gaps exist, technical resource addition plans are outlined below as "First Year New Hires." Resources now in place, shown as "Existing Department Personnel", are employees whose primary responsibility is the registry system.

Software Engineering:

- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- First Year New Hires: Web Developer, Database Engineer, Technical Writer,

Build⁄Deployment Engineer

Systems Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Systems Administrators, two Systems Administrators, two Sr. Systems Engineers, two Systems Engineers
- First Year New Hires: Systems Engineer

Network Engineering:

- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, two Network Engineers
- First Year New Hires: Network Engineer

Database Operations:

- Existing Department Personnel: Sr. Database Operations Manager, two Database Administrators

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information Security Specialist, Information Security Specialists, Sr. Information Security Engineer, Information Security Engineer
- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

- Existing Department Personnel: Manager, two NOC Supervisors, 12 NOC Analysts
- First Year New Hires: Eight NOC Analysts

11.0. PROVISION FOR SEARCHABLE WHOIS CAPABILITIES

The searchable Whois service for our gTLD provides flexible and powerful search ability for users through a web-based interface. This service is provided only to entities with a demonstrated need for it. Where access to registration data is critical to the investigation of cybercrime and other potentially unlawful activity, we authorize access for fully vetted law enforcement and other entities as appropriate. Search capabilities for our gTLD’s searchable Whois meet or exceed the requirements indicated in section 1.8 of specification 4.

Once authorized to use the system, a user can perform exact and partial match searches on the following fields:

- Domain name
- Registrant name
- Postal address including street, city and state, etc., of all registration contacts
- Contact names
- Registrant email address
- Registrar name and ID
- Nameservers
- Internet Protocol addresses

In addition, all other EPP Contact Object fields and sub-fields are searchable as well. The following Boolean operators are also supported: AND, OR, NOT. These operators can be used for joining or excluding results.

Certain types of registry related abuse are unique to the searchable Whois function. Providing searchable Whois warrants providing protection against this abuse. Potential problems include:

- Attempts to abuse Whois by issuing a query that essentially returns the entire database in the result set.
- Attempts to run large quantities of queries sufficient to reduce the performance of the registry database.

Precautions for preventing and mitigating abuse of the Whois search service include:

- Limiting access to authorized users only.
- Establishing legal agreements with authorized users that clearly define and prohibit system abuse.
- Queuing search queries into a job processing system.
- Executing search queries against a replicated read-only copy of the database.
- Limiting result sets when the query is clearly meant to cause a wholesale dump of registration data.

Only authorized users with a legitimate purpose for searching registration data are permitted to use the searchable Whois system. Examples of legitimate purpose include the investigation of terrorism or cybercrime by authorized officials, or any of many other official activities that public officials must conduct to fulfill their respective duties. We grant access for these and other purposes on a case-by-case basis.

To ensure secure access, a two-factor authentication device is issued to each authorized user of the registry. Subsequent access to the system requires the user name, password and a one-time generated password from the issued two-factor device.

Upon account creation, users are provided with documentation describing our terms of service and policies for acceptable use. Users must agree to these terms to use the system. These terms clearly define and illustrate what constitutes legitimate use and what constitutes abuse. They also inform the user that abuse of the system is grounds for limiting or terminating the user’s account.

For all queries submitted, the searchable Whois system first sanitizes the query to deter potential harm to our internal systems. The system then submits the query to a queue for job processing. The system processes each query one by one and in the order received. The number of concurrent queries executed varies, depending on the current load.

To ensure Whois search capabilities do not affect other registry systems, the system executes queries against a replicated read-only version of the database. The system updates this database frequently as registration transactions occur. These updates are performed in a manner that ensures no detrimental load is placed on the production SRS.

To process successfully, each query must contain the criteria needed to filter its results down to a reasonable result set (one that is not excessively large). If the query does not meet this, the user is notified that the result set is excessive and is asked to verify the search criteria. If the user wishes to continue without making the indicated changes, the user must contact our support team to verify and approve the query. Each successful query submitted results in immediate execution of the query.

Query results are encrypted using the unique shared secret built into each 256-bit Advanced Encryption Standard (AES) two-factor device. The results are written to a secure location dedicated for result storage and retrieval. Each result report has a unique file name in the user's directory. The user's directory is assigned the permissions needed to prevent unauthorized access to report files. For the convenience of Registrars and other users, each query result is stored for a minimum of 30 days. At any point following this 30-day period, the query result may be purged by the system.

27. Registration Life Cycle

Q27 CHAR: 19951

1.0. INTRODUCTION
To say that the lifecycle of a domain name is complex would be an understatement. A domain name can traverse many states throughout its lifetime and there are many and varied triggers that can cause a state transition. Some states are triggered simply by the passage of time. Others are triggered by an explicit action taken by the registrant or registrar. Understanding these is critical to the proper operation of a gTLD registry. To complicate matters further, a domain name can contain one or more statuses. These are set by the registrar or registry and have a variety of uses.

When this text discusses EPP commands received from registrars, with the exception of a transfer request, the reader can assume that the command is received from the sponsoring registrar and successfully processed. The transfer request originates from the potential gaining registrar. Transfer details are explicit for clarity.

2.0. INDUSTRY STANDARDS
The registration life cycle approach for our gTLD follows industry standards for registration lifecycles and registration statuses. By implementing a registration life cycle that adheres to these standards, we avoid compounding an already confusing topic for registrants. In addition, since registrar systems are already designed to manage domain names in a standard way, a standardized registration lifecycle also lowers the barrier to entry for registrars.

The registration lifecycle for our gTLD follows core EPP RFCs including RFC 5730 and RFC 5731 and associated documentation of lifecycle information. To protect registrants, EPP Grace Period Mapping for domain registrations is implemented, which affects the registration lifecycle and domain status. EPP Grace Period Mapping is documented in RFC 3915.

3.0. REGISTRATION STATES
For a visual guide to this registration lifecycle discussion, please refer to the attachment, Registration Lifecycle Illustrations. Please note that this text makes many references to the status of a domain. For brevity, we do not distinguish between the domain mapping status 〈domain:status〉 and the EPP Grace Period Mapping status 〈rgp:rgpStatus〉 as making this differentiation in every case would make this document more difficult to read and in this context does not improve understanding.

4.0. AVAILABILITY
The lifecycle for any domain registration begins with the Available state. This is not necessarily a registration state, per se, but indicates the lack of domain registration implied and provides an entry and terminal point for the state diagram

provided. In addition to the state diagram, please refer to Fig. 2 – Availability Check for visual representation of the process flow.

Before a user can register a new domain name, the registry performs an availability check. Possible outcomes of this availability check include:
1. Domain name is available for registration.
2. Domain name is already registered, regardless of the current state and not available for registration.
3. Domain name has been reserved by the registry.
4. Domain name string has been blocked because of a trademark claim.

5.0. INITIAL REGISTRATION
The first step in domain registration is the availability check as described above and shown in Fig. 2 – Availability Check. A visual guide to the description for domain registration in this section can be found in Fig. 3 – Domain Registration. If the domain is available for registration, a registrar submits a registration request.

With this request, the registrar can include zero or more nameserver hosts for zone delegation. If the registrar includes zero or one nameserver host(s), the domain is registered but the EPP status of the domain is set to inactive. If the registrar includes two or more, the EPP status of the domain is set to ok.

The request may also include a registration period (the number of years the registrar would like the domain registered). If this time period is omitted, the registry may use a default initial registration period. The policy for this aligns with the industry standard of one year as the default period. If the registrar includes a registration period, the value must be between one and ten years as specified in the gTLD Registry Agreement.

Once the registration process is complete within the registry, the domain registration is considered to be in the REGISTERED state but within the Add Grace Period.

6.0. REGISTERED STATE - ADD GRACE PERIOD
The Add Grace Period is a status given to a new domain registration. The EPP status applied in this state is addPeriod. The Add Grace Period is a state in which the registrar is eligible for a refund of the registration price should the registration be deleted while this status is applied. The status is removed and the registration transitions from the Add Grace Period either by an explicit delete request from the registrar or by the lapse of five days. This is illustrated in Fig. 1 and Fig. 3 of the illustrations attachment.

If the registrar deletes the domain during the Add Grace Period, the domain becomes immediately available for registration. The registrar is refunded the original cost of the registration.

If the five-day period lapses without receiving a successful delete command, the addPeriod status is removed from the domain.

7.0. REGISTERED STATE
A domain registration spends most of its time in the REGISTERED state. A domain registration period can initially be between one year and ten years in one-year increments as specified in the new gTLD Registry Agreement. At any time during the registration's term, several things can occur to either affect the registration period or transition the registration to another state. The first three are the auto-

renew process, an explicit renew EPP request and a successful completion of the transfer process.

8.0. REGISTRATION PERIOD EXTENSION
The registration period for a domain is extended either through a successful renew request by the registrar, through the successful completion of the transfer process or through the auto-renew process. This section discusses each of these three options.

8.1. EXTENSION VIA RENEW REQUEST
One way that a registrar can extend the registration period is by issuing a renew request. Each renew request includes the number of years desired for extension of the registration up to ten years. Please refer to the flow charts found in both Fig. 4 - Renewal and Fig. 5 - Renewal Grace Period for a visual representation of the following.

Because the registration period cannot extend beyond ten years, any request for a registration period beyond ten years fails. The domain must not contain the status renewProhibited. If this status exists on the domain, the request for a renewal fails.

Upon a successful renew request, the registry adds the renewPeriod status to the domain. This status remains on the domain for a period of five days. The number of years in the renew request is added to the total registration period of the domain. The registrar is charged for each year of the additional period.

While the domain has the renewPeriod status, if the sponsoring registrar issues a successful delete request, the registrar receives a credit for the renewal. The renewPeriod status is removed and the domain enters the Redemption Grace Period (RGP) state. The status redemptionPeriod is added to the status of the domain.

8.2. EXTENSION VIA TRANSFER PROCESS
The second way to extend the registration is through the Request Transfer process. A registrar may transfer sponsorship of a domain name to another registrar. The exact details of a transfer are explained in the Request Transfer section below. The successful completion of the Request Transfer process automatically extends the registration for one year. The registrar is not charged separately for the addition of the year; it comes automatically with the successful transfer. The transferPeriod status is added to the domain.

If the gaining registrar issues a successful delete request during the transferPeriod, the gaining registrar receives a credit for the transfer. The status redemptionPeriod is added to the status of the domain and transferPeriod is removed. The domain then enters the RGP state.

8.3. EXTENSION VIA AUTO-RENEW
The last way a registration period can be extended is passive and is the simplest way because it occurs without any action by the Registrar. When the registration period expires, for the convenience of the registrar and registrant, the registration renews automatically for one year. The registrar is charged for the renewal at this time. This begins the Auto Renew Grace Period. The autoRenewPeriod status is added to the domain to represent this period.

The Auto Renew Grace Period lasts for 45 days. At any time during this period, the Registrar can do one of four things: 1) passively accept the renewal; 2) actively renew (to adjust renewal options); 3) delete the registration; or 4) transfer the registration.

To passively accept the renewal, the registrar need only allow the 45-day time span to pass for the registration to move out of the Auto Renew Grace Period.

Should the registrar wish to adjust the renewal period in any way, the registrar can submit a renew request via EPP to extend the registration period up to a maximum of ten years. If the renew request is for a single year, the registrar is not charged. If the renew request is for more than a single year, the registrar is charged for the additional years that the registration period was extended. If the command is a success, the autoRenewPeriod status is removed from the domain.

Should the registrar wish to delete the registration, the registrar can submit a delete command via EPP. Once a delete request is received, the autoRenewPeriod status is removed from the domain and the redemptionPeriod status is added. The registrar is credited for the renewal fees. For illustration of this process, please refer to Fig. 6 - Auto Renew Grace Period.

The last way move a domain registration out of the Auto Renew state is by successful completion of the Request Transfer process, as described in the following section. If the transfer completes successfully, the autoRenewPeriod status is removed and the transferPeriod status is added.

9.0. REQUEST TRANSFER

A customer can change the sponsoring registrar of a domain registration through the Request Transfer process. This process is an asynchronous, multi-step process that can take many as five days but may occur faster, depending on the level of support from participating Registrars.

The initiation of the transfer process is illustrated in Fig. 8 - Request Transfer. The transfer process begins with a registrar submitting a transfer request. To succeed, the request must meet several criteria. First, the domain status must not contain transferProhibited or pendingTransfer. Second, the initial domain registration must be at least 60 days old or, if transferred prior to the current transfer request, must not have been transferred within the last 60 days. Lastly, the transfer request must contain the correct authInfo (authorization information) value. If all of these criteria are met, the transfer request succeeds and the domain moves into the Pending Transfer state and the pendingTransfer status is added to the domain.

There are four ways to complete the transfer (and move it out of Pending Transfer status):
1. The transfer is auto-approved.
2. The losing registrar approves the transfer.
3. The losing registrar rejects the transfer.
4. The requesting registrar cancels the transfer.

After a successful transfer request, the domain continues to have the pendingTransfer status for up to five days. During this time, if no other action is taken by either registrar, the domain successfully completes the transfer process and the requesting registrar becomes the new sponsor of the domain registration. This is illustrated in Fig. 9 - Auto Approve Transfer.

At any time during the Pending Transfer state, either the gaining or losing registrar can request the status of a transfer provided they have the correct domain authInfo. Querying for the status of a transfer is illustrated in Fig. 13 - Query Transfer.

During the five-day Pending Transfer state, the losing registrar can accelerate the process by explicitly accepting or rejecting the transfer. If the losing registrar takes either of these actions, the pendingTransfer status is removed. Both of these actions are illustrated in Fig. 10 - Approve Transfer and Fig. 11 - Reject Transfer.

During the five-day Pending Transfer state, the requesting registrar may cancel the transfer request. If the registrar sends a cancel transfer request, the pendingTransfer status is removed. This is shown in Fig. 12 - Cancel Transfer.

If the transfer process is a success, the registry adds the transferPeriod status and removes the pendingTransfer status. If the domain was in the Renew Period state, upon successful completion of the transfer process, this status is removed.

The transferPeriod status remains on the domain for five days. This is illustrated in Fig. 14 - Transfer Grace Period. During this period, the gaining Registrar may delete the domain and obtain a credit for the transfer fees. If the gaining registrar issues a successful delete request during the transferPeriod, the gaining registrar receives a credit for the transfer. The status redemptionPeriod is added to the status of the domain and transferPeriod is removed. The domain then enters the RGP state.

10.0. REDEMPTION GRACE PERIOD

The Redemption Grace Period (RGP) is a service provided by the registry for the benefit of registrars and registrants. The RGP allows a registrar to recover a deleted domain registration. The only way to enter the RGP is through a delete command sent by the sponsoring registrar. A domain in RGP always contains a status of redemptionPeriod. For an illustrated logical flow diagram of this, please refer to Fig. 15 - Redemption Grace Period.

The RGP lasts for 30 days. During this time, the sponsoring registrar may recover the domain through a two-step process. The first step is to send a successful restore command to the registry. The second step is to send a restore report to the registry.

Once the restore command is processed, the registry adds the domain status of pendingRestore to the domain. The domain is now in the Pending Restore state, which lasts for seven days. During this time, the registry waits for the restore report from the Registrar. If the restore report is not received within seven days, the domain transitions back to the RGP state. If the restore report is successfully processed by the registry, the domain registration is restored back to the REGISTERED state. The statuses of pendingRestore and redemptionPeriod are removed from the domain.

After 30 days in RGP, the domain transitions to the Pending Delete state. A status of pendingDelete is applied to the domain and all other statuses are removed. This state lasts for five days and is considered a quiet period for the domain. No commands or other activity can be applied for the domain while it is in this state. Once the five days lapse, the domain is again available for registration.

11.0. DELETE

To delete a domain registration, the sponsoring registrar must send a delete request to the registry. If the domain is in the Add Grace Period, deletion occurs immediately. In all other cases, the deleted domain transitions to the RGP. For a detailed visual diagram of the delete process flow, please refer to Fig. 7 - Delete.

For domain registration deletion to occur successfully, the registry must first ensure the domain is eligible for deletion by conducting two checks. The registry first checks to verify that the requesting registrar is also the sponsoring registrar. If this is not the case, the registrar receives an error message.

The registry then checks the various domain statuses for any restrictions that might prevent deletion. If the domain's status includes either the transferPending or deleteProhibited, the name is not deleted and an error is returned to the registrar.

If the domain is in the Add Grace Period, the domain is immediately deleted and any registration fees paid are credited back to the registrar. The domain is immediately available for registration.

If the domain is in the Renew Grace Period, the Transfer Grace Period or the Auto Renew Grace Period, the respective renewPeriod, transferPeriod or autoRenewPeriod statuses are removed and the corresponding fees are credited to the Registrar. The domain then moves to the RGP as described above.

12.0. ADDITIONAL STATUSES

There are additional statuses that the registry or registrar can apply to a domain registration to limit what actions can be taken on it or to limit its usefulness. This section addresses such statuses that have not already addressed in this response.

Some statuses are applied by the registrar and others are exclusively applied by the registry. Registry-applied statuses cannot be altered by registrars. Status names that registrars can add or remove begin with “client”. Status names that only the registry can add or remove begin with “server”. These statuses can be applied by a registrar using the EPP domain update request as defined in RFC 5731.

To prevent a domain registration from being deleted, the status values of clientDeleteProhibited or serverDeleteProhibited may be applied by the appropriate party.

To withhold delegation of the domain to the DNS, clientHold or serverHold is applied. This prevents the domain name from being published to the zone file. If it is already published, the domain name is removed from the zone file.

To prevent renewal of the domain registration clientRenewProhibited or serverRenewProhibited is applied by the appropriate party.

To prevent the transfer of sponsorship of a registration, the states clientTransferProhibited or serverTransferProhibited is applied to the domain. When this is done, all requests for transfer are rejected by the registry.

If a domain registration contains no host objects, the registry applies the status of inactive. Since there are no host objects associated with the domain, by definition, it cannot be published to the zone. The inactive status cannot be applied by registrars.

If a domain has no prohibitions, restrictions or pending operations and the domain also contains sufficient host object references for zone publication, the registry assigns the status of ok if there is no other status set.

There are a few statuses defined by the domain mapping RFC 5731 that our registry does not use. These statuses are: pendingCreate, pendingRenew and pendingUpdate. RFC 5731 also defines some status combinations that are invalid. We acknowledge these and our registry system disallows these combinations.

13.0. RESOURCING
Software Engineering:
- Existing Department Personnel: Project Manager, Development Manager, two Sr. Software Engineers, Sr. Database Engineer, Quality Assurance Engineer
- New Hires: Web Developer, Database Engineer, Technical Writer, Build⁄Deployment Engineer
Systems Engineering:
- Existing Department Personnel: Sr. Director IT Operations, 2 Sr. Systems Administrators, 2 Systems Administrators, 2 Sr. Systems Engineers, 2 Systems Engineers
- New Hires: Systems Engineer
Network Engineering:
- Existing Department Personnel: Sr. Director IT Operations, two Sr. Network Engineers, 2 Network Engineers
- New Hires: Network Engineer
Database Operations:
- Existing Department Personnel: Sr. Database Operations Manager, 2 Database Administrators
Network Operations Center:
- Existing Department Personnel: Manager, 2 NOC Supervisors, 12 NOC Analysts
- New Hires: Eight NOC Analysts

28. Abuse Prevention and Mitigation

Q28 SV CHAR: 30317

1.0. INTRODUCTION

Donuts will employ strong policies and procedures to prevent and mitigate abuse. Our intention is to ensure the integrity of this top-level domain (TLD) and maintain it as a trusted space on the Internet. We will not tolerate abuse and will use professional, consistent, and fair policies and procedures to identify and address abuse in the legal, operational, and technical realms

Our approach to abuse prevention and mitigation includes the following:

- An Anti-Abuse Policy that clearly defines malicious and abusive behaviors;
- An easy-to-use single abuse point of contact (APOC) that Internet users can use to report the malicious use of domains in our TLD;
- Procedures for investigating and mitigating abuse;
- Procedures for removing orphan glue records used to support malicious activities;
- Dedicated procedures for handling legal requests, such as inquiries from law enforcement bodies, court orders, and subpoenas;
- Measures to deter abuse of the Whois service; and
- Policies and procedures to enhance Whois accuracy, including compliance and monitoring programs.

Our abuse prevention and mitigation solution leverages our extensive domain name industry experience and was developed based on extensive study of existing gTLDs and ccTLDs for best registry practices. This same experience will be leveraged to manage the new TLD.

2.0. ANTI-ABUSE POLICY

The Anti-Abuse Policy for our registry will be enacted under the Registry-Registrar Agreement, with obligations from that agreement passed on to and made binding upon all registrants, registrars, and resellers. This policy will also be posted on the registry web site and accompanied by abuse point-of-contact contact information (see below). Internet users can report suspected abuse to the registry and sponsoring registrar, and report an orphan glue record suspected of use in connection with malicious conduct (see below).

The policy is especially designed to address the malicious use of domain names. Its intent is to:

1. Make clear that certain types of behavior are not tolerated;
2. Deter both criminal and non-criminal but harmful use of domain names; and
3. Provide the registry with clearly stated rights to mitigate several types of abusive behavior when found.

This policy does not take the place of the Uniform Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism.

Below is a policy draft based on the anti-abuse policies of several existing TLD registries with exemplary practices (including .ORG, .CA, and .INFO). We plan to adopt the same, or a substantially similar version, after the conclusion of legal reviews.

3.0. TLD ANTI-ABUSE POLICY

The registry reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, redirect, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any of the following reasons:

(1) to protect the integrity and stability of the registry;
(2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
(3) to avoid any liability, civil or criminal, on the part of the registry operator, its affiliates, subsidiaries, officers, directors, or employees;
(4) to comply with the terms of the registration agreement and the registry’s Anti-Abuse Policy;
(5) registrant fails to keep Whois information accurate and up-to-date;
(6) domain name use violates the registry’s acceptable use policies, or a third party’s rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;
(7) to correct mistakes made by the registry operator or any registrar in connection with a domain name registration; or
(8) as needed during resolution of a dispute.

Abusive use of a domain is an illegal, malicious, or fraudulent action and includes, without limitation, the following:

- Distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include computer viruses, worms, keyloggers, trojans, and fake antivirus products;
- Phishing: attempts to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication;
- DNS hijacking or poisoning;

- Spam: The use of electronic messaging systems to send unsolicited bulk messages. This includes but is not limited to email spam, instant messaging spam, mobile messaging spam, and the spamming of Internet forums;
- Use of botnets, including malicious fast-flux hosting;
- Denial-of-service attacks;
- Child pornography⁄child sexual abuse images;
- The promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law; and
- Illegal access of computers or networks.

4.0. SINGLE ABUSE POINT OF CONTACT

Our prevention and mitigation plan includes use of a single abuse point of contact (APOC). This contact will be a role-based e-mail address in the form of “abuse@registry.tld”. This e-mail address will allow multiple staff members to monitor abuse reports. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered an Internet abuse desk best practice.

The APOC e-mail address will be listed on the registry web site. We also will provide a convenient web form for complaints. This form will prompt complainants to provide relevant information. (For example, complainants who wish to report spam will be prompted to submit the full header of the e-mail.) This will help make their reports more complete and accurate.

Complaints from the APOC e-mail address and web form will go into a ticketing system, and will be routed to our abuse handlers (see below), who will evaluate the tickets and execute on them as needed.

The APOC is mainly for complaints about malicious use of domain names. Special addresses may be set up for other legal needs, such as civil and criminal subpoenas, and for Sunrise issues.

5.0. ABUSE INVESTIGATION AND MITIGATION

Our designated abuse handlers will receive and evaluate complaints received via the APOC. They will decide whether a particular issue merits action, and decide what action is appropriate.

Our designated abuse handlers have domain name industry experience receiving, investigating and resolving abuse reports. Our registry implementation plan will leverage this experience and deploy additional resources in an anti-abuse program tailored to running a registry.

We expect that abuse reports will be received from a wide variety of parties, including ordinary Internet users; security researchers and Internet security companies; institutions, such as banks; and law enforcement agencies.

Some of these parties typically provide good forensic data or supporting evidence of the alleged malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide evidence. It is not unusual, in the Internet industry, that a certain percentage of abuse reports are not actionable because there is insufficient evidence to support the complaint, even after additional investigation.

The abuse handling function will be staffed with personnel who have experience handling abuse complaints. This group will function as an abuse desk to “triage” and investigate reports. Over the past several years, this group has investigated allegations about a variety of problems, including malware, spam, phishing, and child pornography⁄child sexual abuse images.

6.0. POLICIES, PROCEDURES, AND SERVICE LEVELS

Our abuse prevention and mitigation plan includes development of an internal manual for assessing and acting upon abuse complaints. Our designated abuse handlers will use this to ensure consistent and fair processes. To prevent exploitation of internal procedures by malefactors, these procedures will not be published publicly.

Assessing abuse reports requires great care. The goals are accuracy, a zero false-positive rate to prevent harm to innocent registrants, and good documentation.

Different types of malicious activities require different methods of investigation and documentation. The procedures we deploy will address all the abuse types listed in our Anti-Abuse Policy (above). This policy will also contain procedures for assessing complaints about orphan nameservers used for malicious activities.

One of the first steps in addressing abusive or harmful activities is to determine the type of domain involved. Two types of domains may be involved: 1) a “compromised domain”; and⁄or 2) a maliciously registered domain.

A “compromised” domain is one that has been hacked or otherwise compromised by criminals; the registrant is not responsible for the malicious activity taking place on the domain. For example, most domain names that host phishing sites are compromised. The goal in such cases is to inform the registrant of the problem via the registrar. Ideally, such domains are not suspended, since suspension disrupts legitimate activity on the domain.

The second type of potentially harmful domain, the maliciously registered domain, is one registered by a bad actor for the purpose of abuse. Since it has no legitimate use, this type of domain is a candidate for suspension.

In general, we see the registry as the central entity responsible for monitoring abuse of the TLD and passing any complaints received to the domains’ sponsoring registrars. In an alleged (though credible) case of malicious use, the case will be communicated to the domain’s sponsoring registrar requesting that the registrar investigate, act appropriately, and report on it within a defined time period. Our abuse handlers will also provide any evidence they collect to the registrar.

There are several good reasons for passing a case of malicious domain name use on to the registrar. First, the registrar has a direct relationship and contract with the registrant. It is important to respect this relationship as it pertains both to business in general and any legal perspectives involved. Second, the registrar holds a better position to evaluate and act because the registrar typically has vital information the registry operator does not, including domain purchase details and payment method (i.e., credit card, etc.); the identity of a proxy-protected registrant; the IP address from which the domain purchase was made; and whether a reseller is involved. Finally, it is important the registrar know if a registrant is in violation of registry or registrar policies and terms—the registrar may wish to suspend the registrant’s account, or investigate other domains the registrar has registered in this TLD or others.

The registrar is also often best for determining if questionable registrant activity violates the registrar’s legal terms of service or the registry Anti-Abuse Policy, and deciding whether to take any action. Registrars will be required to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action and allows the registrar to suspend or cancel a domain name.

If a registrar does not take action within the time indicated by us in the report (i.e., 24 hours), we may take action ourselves. In some cases, we may suspend the domain name(s), and we reserve the right to act directly and immediately. We plan to take action directly if time is of the essence, such as with a malware attack that may cause significant harm to Internet users.

It is important to note that strict service level agreements (SLAs) for abuse response and mitigation are not always appropriate, additional tailoring of any SLAs may be required, depending on the problem. For example, suspending a domain within 24 hours may not be the best course of action when working with law enforcement or a national clearinghouse to address reports of child pornography. Officials may need more than 24 hours to investigate and gather evidence.

7.0. ABUSE MONITORING AND METRICS

In addition to addressing abuse complaints, we will actively monitor the overall abuse status of the TLD, gather intelligence and track abuse metrics to address criminal use of domains in the TLD.

To enable active reporting of problems to the sponsoring registrars, our plan includes proactive monitoring for malicious use of the domains in the TLD. Our goal is to keep malicious activity at an acceptably low level, and mitigate it actively when it occurs—we may do so by using professional blocklists of domain names. For example, professional advisors such as LegitScript (www.legitscript.com) may be used to identify and close down illegal “rogue” Internet pharmacies.

Our approach also incorporates recordkeeping and metrics regarding abuse and abuse reports. These may include:

- The number of abuse reports received by the registry’s abuse point of contact described above and the domains involved;
- The number of cases and domains referred to registrars for resolution;
- The number of cases and domains for which the registry took direct action;
- Resolution times (when possible or relevant, as resolution times for compromised domains are difficult to measure).

We expect law enforcement to be involved in only a small percentage of abuse cases and will call upon relevant law enforcement as needed.

8.0. HANDLING REPORTS FROM LAW ENFORCEMENT, COURT ORDERS

The new gTLD Registry Agreement contains this requirement: “Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.” (Article 2.8)

We will be responsive as required by Article 2.8. Our abuse handling team will comply with legal processes and leverage both experience and best practices to work effectively with law enforcement and other government agencies. The registry will post a Criminal Subpoena Policy and Procedure page, which will detail how law enforcement and government agencies may submit criminal and civil subpoenas. When we receive valid court orders or seizure warrants from courts or law enforcement agencies of relevant jurisdiction, we will expeditiously review and comply with them.

9.0. PROHIBITING DOMAIN HIJACKINGS AND UNAPPROVED UPDATES

Our abuse prevention and mitigation plan also incorporates registrars that offer domain protection services and high-security access and authentication controls. These include services designed to prevent domain hijackings and inhibit unapproved updates (such as malicious changes to nameserver settings). Registrants will then have the opportunity to obtain these services should they so elect.

10.0. ABUSE POLICY: ADDRESSING INTELLECTUAL PROPERTY INFRINGEMENT

Intellectual property infringement involves three distinct but sometimes intertwined problems: cybersquatting, piracy, and trademark infringement:

- Cybersquatting is about the presence of a trademark in the domain string itself.
- Trademark infringement is the misuse or misappropriation of trademarks - the violation of the exclusive rights attached to a trademark without the authorization of the trademark owner or any licensees. Trademark infringement sometimes overlaps with piracy.
- Piracy involves the use of a domain name to sell unauthorized goods, such as copyrighted music, or trademarked physical items, such as fake brand-name handbags. Some cases of piracy involve trademark infringement.

The Uniform Dispute Resolution Process (UDRP) and the new Uniform Rapid Suspension System (URS) are anti-cybersquatting policies. They are mandatory and all registrants in the new TLD will be legally bound to them. Please refer to our response to Question #29 for details on our plans to respond to URS orders.

The Anti-Abuse Policy for our gTLD will be used to address phishing cases that involve trademarked strings in the domain name. The Anti-Abuse Policy prohibits violation of copyright or trademark; such complaints will be routed to the sponsoring Registrar.

11.0. PROPOSED MEASURES FOR REMOVAL OF ORPHAN GLUE RECORDS

Below are the policies and procedures to be used for our registry in handling orphan glue records. The anti-abuse documentation for our gTLD will reflect these procedures.

By definition, a glue record becomes an "orphan" when the delegation point Name Server (NS) record referencing it is removed without also removing the corresponding glue record. The delegation point NS record is sometimes referred to as the parent NS record.

As ICANN’s SSAC noted in its Advisory SAC048 “SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook” (http://www.icann.org/en/committees/security/sac048.pdf), "Orphaned glue can be used for abusive purposes; however, the dominant use of orphaned glue supports the correct and ordinary operation of the Domain Name System (DNS)." For example, orphan glue records may be created when a domain (example.tld) is placed on Extensible Provisioning Protocol (EPP) ServerHold or ClientHold status. This use of Hold status is an essential tool for suspending malicious domains. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve.

We will use the following procedure—used by several existing registries and considered a generally accepted DNS practice—to manage orphan glue records.. When a registrar submits a request to delete a domain, the registry first checks for the existence of glue records. If glue records exist, the registry checks to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records, then registrar EPP requests to delete the domain will fail until no other domains are using the glue records. (This functionality is currently in place for the .ORG registry.) However, if a registrar submits a complaint that orphan glue is being used maliciously and the malicious conduct is confirmed, the registry operator will remove the orphan glue record from the zone file via an exceptional process.

12.0. METHODS TO PROMOTE WHOIS ACCURACY

12.1. ENFORCING REQUIRED CONTACT DATA FIELDS

We will offer a "thick" registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows for better access to domain data and provides uniformity in storing the information.

As per the EPP specification, certain contact data fields are mandatory. Our registry will enforce those, plus certain other fields as necessary. This ensures that registrars are providing required domain registration data. The following fields (indicated as "MANDATORY") will be mandatory at a minimum:

Contact Name [MANDATORY]
Street1 [MANDATORY]
City [MANDATORY]
State⁄Province [optional]
Country [MANDATORY]
Postal Code [optional]
Registrar Phone [MANDATORY]
Phone Ext [optional]
Fax [optional]
Fax Ext [optional]
Email [MANDATORY]

In addition, our registry will verify formats for relevant individual data fields (e.g. e-mail, and phone⁄fax numbers) and will reject any improperly formatted submissions. Only valid country codes will be allowed, as defined by the ISO 3166 code list.

We will reject entries that are clearly invalid. For example, a contact that contains phone numbers such as 555.5555, or registrant names that consist only of hyphens, will be rejected.

12.2. POLICIES AND PROCEDURES TO ENHANCE WHOIS ACCURACY COMPLIANCE

We generally will rely on registrars to enforce WHOIS accuracy measures, but will also rely on review and audit procedures to enhance compliance.

As part of our RRA (Registry-Registrar Agreement), we will require each registrar to be responsible for ensuring the input of accurate Whois data by its registrants. The Registrar⁄Registered Name Holder Agreement will include specific clauses to ensure accuracy of Whois data, as per ICANN requirements, and to give the registrar the right to cancel or suspend registrations if the registered name holder fails to respond to the registrar’s query regarding accuracy of data. In addition, the Anti-Abuse Policy for our registry will give the registry the right to suspend, cancel, etc., domains that have invalid Whois data.

As part of our RRA (Registry-Registrar Agreement), we will include a policy similar to the one below, currently used by the Canadian Internet Registration Authority (CIRA), the operator of the .CA registry. It will require the registrar to help us verify contact data.

“CIRA is entitled at any time and from time to time during the Term…to verify: (a) the truth, accuracy and completeness of any information provided by the Registrant to CIRA, whether directly, through any of the Registrars of Record or otherwise; and (b) the compliance by the Registrant with the provisions of the Agreement and the Registry PRP. The Registrant shall fully and promptly cooperate with CIRA in connection with such verification and shall give to CIRA, either directly or through the Registrar of Record such assistance, access to and copies of, such information and documents as CIRA may reasonably require to complete such verification. CIRA and the Registrant shall each be responsible for their own expenses incurred in connection with such verification.”
http:⁄⁄www.cira.ca⁄assets⁄Documents⁄Legal⁄Registrants⁄registrantagreement.pdf

On a periodic basis, we will perform spot audits of the accuracy of Whois data in the registry. Questionable data will be sent to the sponsoring registrars as per the above policy.

All accredited registrars have agreed with ICANN to obtain contact information from registrants, and to take reasonable steps to investigate and correct any reported inaccuracies in contact information for domain names registered through them. As part of our RRA (Registry-Registrar Agreement), we will include a policy that allows us to de-accredit any registrar who a) does not respond to our Whois accuracy requests, or b) fails to update Whois data or delete the name within 15 days of our report of invalid WHOIS data. In order to allow for inadvertent and unintentional mistakes by a registrar, this policy may include a “three strikes” rule under which a registrar may be de-accredited after three failures to comply.

12.3. PROXY⁄PRIVACY SERVICE POLICY TO CURB ABUSE

In our TLD, we will allow the use of proxy⁄privacy services. We believe that there are important, legitimate uses for such services. (For example, to protect free speech rights and avoid receiving spam.)

However, we will limit how proxy⁄privacy services are offered. The goal of this policy is to make proxy⁄privacy services unattractive to abusers, namely the spammers and e-criminals who use such services to hide their identities. We believe the policy below will enhance WHOIS accuracy, will help deter the malicious use of domain names in our TLD, and will aid in the investigation and mitigation of abuse complaints.

Registry policy will require the following, and all registrars and their registrants and resellers will be bound to it contractually:

a. Registrants must provide complete and accurate contact information to their registrar (or reseller, if applicable).. Domains that do not meet this policy may be suspended.
b. Registrars and resellers must provide the underlying registrant information to the registry operator, upon written request, during an abuse investigation. This information will be held in confidence by the registry operator.
c. The registrar or reseller must publish the underlying registrant information in

the Whois if it is determined by the registry operator or the registrar that the registrant has breached any terms of service, such as the TLD Anti-Abuse Policy.

The purpose of the above policy is to ensure that, in case of an abuse investigation, the sponsoring registrar has access to the registrant’s true identity, and can provide that data to the registry. If it is clear the registrant has violated the TLD’s Anti-Abuse Policy or other terms of service, the registrant’s identity will be published publicly via the Whois, where it can be seen by the public and by law enforcement.

13.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO ABUSE

Donuts does not currently intend to become a registrar for this TLD. Donuts and our back-end technical operator will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9. For abuse issues, we will comply by establishing an adequate “firewall” between our registry operations and the operations of any affiliated registrar. As the Code requires, the registry will not “directly or indirectly show any preference or provide any special consideration to any Registrar with respect to operational access to registry systems and related registry services”. Here is a non-exhaustive list of specific steps to be taken to enforce this:

- Abuse complaints and cases will be evaluated and executed upon using the same criteria and procedures, regardless of a domain’s sponsoring registrar.
- Registry personnel will not discuss abuse cases with non-registry personnel or personnel from separate entities operating under the company. This policy is designed to both enhance security and prevent conflict of interest.
- If a compliance function is involved, the compliance staff will have responsibilities to the registry only, and not to a registrar we may be “affiliated” with at any point in the future. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that person will have no duty to any registrar business we may be operating at the time. The person will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry impartially and effectively.

14.0. CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS

Our registry incorporates several measures to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, SSL certificates, and proper authentication will be used to control registrar access to the registry system. Registrars will be given access only to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code as per EPP RFCs. The AUTH-INFO code is a 6- to 16-character code assigned by the registrar at the time the name is created. Its purpose is to aid identification of the domain owner so proper authority can be established. (It is the "password" to the domain name.) Registrars must use the domain’s password to initiate a Registrar-to-Registrar transfer. It is used to ensure that domain updates (update contact information, transfer, or deletion) are undertaken by the proper registrant, and that this registrant is adequately notified of domain update activity. Only the sponsoring Registrar of a domain has access to the domain’s AUTH-INFO code stored in the registry, and this is accessible only via encrypted, password-protected channels.

Our Registry-Registrar contract will require that each registrar assign a unique AUTH-INFO code to every domain it creates. Due to security risk, registrars should not assign the same AUTH-INFO code to multiple domains.

Information about other registry security measures such as encryption and security of Registrar channels are confidential to ensure the security of the registry system. Details can be found in our response to Question #30(b).

15.0 ADDITIONAL PROTECTIONS

Due to the level of end-user trust potentially associated with this string Donuts will employ these additional four protections to minimize abuse:

1. For this string, to supplement the periodic audit documented above, a deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes;

2. Exclusion of registrars with a history of poor compliance;

3. Regular monitoring by the registry of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes; and

4. In addition to registry-based procedures, requirements that registrars have a 24⁄7⁄365 abuse contact, and remediation and takedown processes.

16.0. RESOURCING PLAN

Our back-end registry operator will perform the majority of Abuse Prevention and Mitigation services for this TLD, as required by our agreement with them. Donuts staff will supervise the activity of the provider. In some cases Donuts staff will play a direct role in the handling of abuse cases.

The compliance department of our registry operator has two full time staff members who are trained in DNS, the investigation of abuse complaints, and related specialties. The volume of abuse activity will be gauged and additional staff hired by our back-end registry operator as required to meet their SLA commitments. In addition to the two full-time members, they expect to retain the services of one or more outside contractors to provide additional security and anti-abuse expertise – including advice on the effectiveness of our policies and procedures.

Finally, Donuts’ Legal Department will have one attorney whose role includes the oversight of legal issues related to abuse, and interaction with courts and law enforcement.

29. Rights Protection Mechanisms

Q29 SV CHAR: 25795

1.0. INTRODUCTION

To minimize abusive registrations and other activities that affect the legal rights of others, our approach includes well-developed policies for rights protection, both during our TLD’s rollout period and on an ongoing basis. As per gTLD Registry

Agreement Specification 7, we will offer a Sunrise Period and a Trademark Claims service during the required time periods, we will use the Trademark Clearinghouse, and we will implement Uniform Rapid Suspension (URS) on an ongoing basis. In addition to these newly mandated ICANN protections, we will implement two other trademark protections that were developed specifically for the new TLD program. These additional protections are: (i) a Domain Protected Marks List (DPML) for the blocking of trademarked strings across multiple TLDs; and (ii) a Claims Plus product to alert registrars to registrations that potentially infringe existing marks.

Below we detail how we will fulfill these requirements and further meet or exceed ICANN’s requirements. We also describe how we will provide additional measures specific to rights protection above ICANN’s minimum, including abusive use policies, takedown procedures, and other covenants.

Our RPM approach leverages staff with extensive experience in a large number of gTLD and ccTLD rollouts, including the Sunrises for .CO, .MOBI, .ASIA, .EU, .BIZ, .US., .TRAVEL, TEL, .ME, and .XXX. This staff will utilize their first-hand, practical experience and will effectively manage all aspects of Sunrise, including domain application and domain dispute processes.

The legal regime for our gTLD will include all of the ICANN-mandated protections, as well as some independently developed RPMs proactively included in our Registry-Registrar Agreement. Our RPMs exceed the ICANN-required baseline. They are:

- Reserved names: to protect names specified by ICANN, including the necessary geographic names.
- A Sunrise Period: adhering to ICANN requirements, and featuring trademark validation via the Trademark Clearinghouse.
- A Trademark Claims Service: offered as per ICANN requirements, and active after the Sunrise period and for the required time during wider availability of the TLD.
- Universal Rapid Suspension (URS)
- Uniform Dispute Resolution Process (UDRP)
- Domain Protected Marks List (DPML)
- Claims Plus
- Abusive Use and Takedown Policies

2.0. NARRATIVE FOR Q29 FIGURE 1 OF 1

Attachment A, Figure 1, shows Rollout Phases and the RPMs that will be used in each. As per gTLD Registry Agreement Specification 7, we will offer a Sunrise Period and a Trademark Claims service during the required time periods. In addition, we will use the Trademark Clearinghouse to implement URS on an ongoing basis.

3.0. PRE-SUNRISE: RESERVED AND PREMIUM NAMES

Our Pre-sunrise phase will include a number of key practices and procedures. First, we will reserve the names noted in the gTLD Registry Agreement Specification 5. These domains will not be available in Sunrise or subsequent registration periods. As per Specification 5, Section 5, we will provide national governments the opportunity to request the release of their country and territory names for their use. Please also see our response to Question 22, “Protection of Geographic Names.”

We also will designate certain domains as “premium” domains. These will include domains based on generic words and one-character domains. These domains will not be available in Sunrise, and the registry may offer them via special means such as auctions and RFPs.

As an additional measure, if a trademark owner objects to a name on the premium name list, the trademark owner may petition to have the name removed from the list and made available during Sunrise. The trademark must meet the Sunrise eligibility rules (see below), and be an exact match for the domain in question. Determinations of whether such domains will be moved to Sunrise will be at the registry's sole discretion.

4.0. SUNRISE

4.1. SUNRISE OVERVIEW

Sunrise registration services will be offered for a minimum of 30 days during the pre-launch phase. We will notify all relevant trademark holders in the Trademark Clearinghouse if any party is seeking a Sunrise registration that is an identical match to the name to be registered during Sunrise.

As per the Sunrise terms, affirmed via the Registry-Registrar Agreement and the Registrar-Registrant Agreement, the domain applicant will assert that it is qualified to hold the domain applied for as per the Sunrise Policy and Rules.

We will use the Trademark Clearinghouse to validate trademarks in the Sunrise.

If there are multiple valid Sunrise applications for the same domain name string, that string will be subject to auction between only the validated applicants. After receipt of payment from the auction winning bidder, that party will become the registrant of the domain name. (note: in the event one of the identical, contending marks is in a trademark classification reflective of the TLD precedence to that mark may be given during Sunrise).

Sunrise applicants may not use proxy services during the application process.

4.2. SUNRISE: ELIGIBLE RIGHTS

Our Sunrise Eligibility Requirements (SERs) are:

1. Ownership of a qualifying mark.

a. We will honor the criteria in ICANN's Trademark Clearinghouse document section 7.2, number (i): The registry will recognize and honor all word marks that are nationally or regionally [see Endnote 1] registered and for which proof of use — which can be a declaration and a single specimen of current use - was submitted to, and validated by, the Trademark Clearinghouse.

b. In addition, we may accept marks that are not found in the Trademark Clearinghouse, but meet other criteria, such as national trademark registrations or common law rights.

2. Representation by the applicant that all provided information is true and correct; and

3. Provision of data sufficient to document rights in the trademark. (See information about required Sunrise fields, below).

4.3. SUNRISE TRADEMARK VALIDATION

Our goal is to award Sunrise names only to applicants who are fully qualified to have them. An applicant will be deemed to be qualified if that applicant has a trademark that meets the Sunrise criteria, and is seeking a domain name that matches that trademark, as per the Sunrise rules.

Accordingly, we will validate applications via the Trademark Clearinghouse. We will compare applications to the Trademark Clearinghouse database, and those that match (as per the Sunrise rules) will be considered valid applications.

An application validated according to Sunrise rules will be marked as “validated,” and will proceed. (See “Contending Applications,” below.) If an application does not qualify, it will be rejected and will not proceed.

To defray the costs of trademark validation and the Trademark Claims Service, we will charge an application and⁄or validation fee for every application.

In January 2012, the ICANN board was briefed that “An ICANN cross-functional team is continuing work on implementation of the Trademark Clearinghouse according to a project plan providing for a launch of clearinghouse operations in October 2012. This will allow approximately three months for rights holders to begin recording trademark data in the Clearinghouse before any new gTLDs begin accepting registrations (estimated in January 2013).” (http:⁄⁄www.icann.org⁄en⁄minutes⁄board-briefing-materials-4-05jan12-en.pdf) The Clearinghouse Implementation Assistance Group (IAG), which Donuts is participating in, is working through a large number of process and technical issues as of this writing. We will follow the progress of this work, and plan our implementation details based on the final specifications.

Compliant with ICANN policy, our registry software is designed to properly check domains and compare them to marks in the Clearinghouse that contain punctuation, spaces, and special symbols.

4.5. CONTENDING APPLICATIONS, SUNRISE AUCTIONS

After conclusion of the Sunrise Period, the registry will finish the validation process. If there is only one valid application for a domain string, the domain will be awarded to that applicant. If there are two or more valid applications for a domain string, only those applicants will be invited to participate in a closed auction for the domain name. The domain will be awarded to the auction winner after payment is received.

After a Sunrise name is awarded to an applicant, it will then remain under a “Sunrise lock” status for a minimum of 60 days in order to allow parties to file Sunrise Challenges (see below). Locked domains cannot be updated, transferred, or deleted.

When a domain is awarded and granted to an applicant, that domain will be available for lookup in the public Whois. Any party may then see what domains have been awarded, and to which registrants. Parties will therefore have the necessary information to consider Sunrise Challenges.

Auctions will be conducted by very specific rules and ethics guidelines. All employees, partners, and contractors of the registry are prohibited from participating in Sunrise auctions.

4.6. SUNRISE DISPUTE RESOLUTION PROCESS (SUNRISE CHALLENGES)

We will retain the services of a well-known dispute resolution provider (such as

WIPO) to help formulate the language of our Sunrise Dispute Resolution Process (SDRP, or “Sunrise Challenge”) and hear the challenges filed under it. All applicants and registrars will be contractually obligated to follow the decisions handed down by the dispute resolution provider.

Our SDRP will allow challenges based on the following grounds, as required by ICANN. These will be part of the Sunrise eligibility criteria that all registrants (applicants) will be bound to contractually:

(i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty;

(ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration;

(iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or

(iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

Our SDRP will be based generally on some SDRPs that have been used successfully in past TLD launches. The Sunrise Challenge Policies and Rules used in the .ASIA and .MOBI TLDs (minus their unique eligibility criteria) are examples.

We expect that that there will be three possible outcomes to a Sunrise Challenge:

1. Original registrant proves his⁄her right to the domain. In this case the registrant keeps the domain and it is unlocked for his⁄her use.
2. Original registrant is not eligible or did not respond, and the challenger proved his⁄her right to the domain. In this case the domains is awarded to the complainant.
3. Neither the original registrant nor the complainant proves rights to the domain. In this case the domain is cancelled and becomes available at a later date via a mechanism to be determined by the registry operator.

After any Sunrise name is awarded to an applicant, it will remain under a “Sunrise Lock” status for at least 60 days so that parties can file Sunrise Challenges. During this Sunrise Lock period, the domain will not resolve and cannot be modified, transferred, or deleted by the sponsoring registrar. A domain name will be unlocked at the end of that lock period only if it is not subject to a Sunrise Challenge. Challenged domains will remain locked until the dispute resolution provider has issued a decision, which the registry will promptly execute.

5.0. TRADEMARK CLAIMS SERVICES

The Trademark Claims Service requirements are well-defined in the Applicant Guidebook, in Section 6 of the “Trademark Clearinghouse” attachment. We will comply with the details therein. We will provide Trademark Claims services for marks in the Trademark Clearinghouse post-Sunrise and then for at least the first 60 days that the registry is open for general registration (i.e. during the first 60 days in the registration period(s) after Sunrise). The Trademark Claims service will provide clear notice to a prospective registrant that another party has a trademark in the Clearinghouse that matches the applied-for domain name—this is a notice to the prospective registrant that it might be infringing upon another party’s rights.

The Trademark Clearinghouse database will be structured to report to registries when registrants are attempting to register a domain name that is considered an “Identical Match” with the mark in the Clearinghouse. We will build, test, and implement an interface to the Trademark Clearinghouse before opening our Sunrise period. As domain name applications come into the registry, those strings will be compared to the contents of the Clearinghouse.

If the domain name is registered in the Clearinghouse, the registry will promptly notify the applicant. We will use the notice form specified in ICANN’s Module 4, “Trademark Clearinghouse” document. The specific statement by the prospective registrant will warrant that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the notice; and (iii) to the best of the prospective registrant’s knowledge, the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice.

The Trademark Claims Notice will provide the prospective registrant access to the Trademark Clearinghouse Database information referenced in the Trademark Claims Notice. The notice will be provided in real time (or as soon as possible) without cost to the prospective registrant or to those notified.

“Identical Match” is defined in ICANN’s Module 4, “Trademark Clearinghouse” document, paragraph 6.1.5. We will examine the Clearinghouse specifications and protocol carefully when they are published. To comply with ICANN policy, the software for our registry will properly check domains and compare them to marks in the Clearinghouse that contain punctuation, spaces, and special symbols.

6.0. GENERAL REGISTRATION

This is the general registration period open to all registrants. No trademark or other qualification will be necessary in order to apply for a domain in this period.

Domain names awarded via the Sunrise process, and domain strings still being contended via the Sunrise process cannot be registered in this period. This will protect the interests of all Sunrise applicants.

7.0. UNIFORM RAPID SUSPENSION (URS)

We will implement decisions rendered under the URS on an ongoing basis. (URS will not apply to Sunrise names while they are in Sunrise Lock period; during that time those domains are subject to Sunrise policy and Sunrise Challenge instead.)

As per URS policy, the registry will receive notice of URS actions from ICANN-approved URS providers. As per ICANN’s URS requirements, we will lock the domain within 24 hours of receipt of the Notice of Complaint from the URS Provider. Locking means that the registry restricts all changes to the registration data, including transfer and deletion of domain names, though names will continue to resolve.

Our registry’s compliance team will oversee URS procedures. URS e-mails from URS providers will be directed immediately to the registry’s Support staff, which is on duty 24⁄7⁄365. Support staff will be responsible for executing the directives from the URS provider, and all support staff will receive training in the proper procedures.

Support staff will notify the URS Provider immediately upon locking the domain name, via e-mail.

Support staff for the registry will retain all copies of e-mails from the URS providers. Each case or order will be assigned a tracking or ticket number. This number will be used to track the status of each opened URS case through to resolution via a database.

Registry staff will then execute further operations upon notice from the URS providers. Each URS provider is required to specify the remedy and required actions of the registry, with notification to the registrant, the complainant, and the sponsoring registrar.

The guidelines provide that if the complainant prevails, the registry "shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS Provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original Registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration." We will execute the DNS re-pointing required by the URS guidelines, and the domain and its WHOIS data will remain unaltered until the domain expires, as per the ICANN requirements.

8.0. ONGOING RIGHTS PROTECTION MECHANISMS - UDRP

As per ICANN policy, all domains in the TLD will be subject to a Uniform Dispute Resolution Process (UDRP). (Sunrise domains will first be subject to the ICANN-mandated Sunrise SDRP until the Sunrise Challenge period is over, after which those domains will then be subject to UDRP.)

9.0 ADDITIONAL RIGHTS PROTECTION MECHANISMS NOT REQUIRED BY ICANN

All Donuts TLDs have two new trademark protection mechanisms developed specifically for the new TLD program. These mechanisms exceed the extensive protections mandated by ICANN. These new protections are:

9.1 Claims Plus: This service will become available at the conclusion of the Trademark Claims service, and will remain available for at least the first five years of registry operations. Trademark owners who are fully registered in the Trademark Clearinghouse may obtain Claims Plus for their marks. We expect the service will be at low or no cost to trademark owners (contingent on Trademark Clearinghouse costs to registries). Claims Plus operates much like Trademark Claims with the exception that notices of potential trademark infringement are sent by the registry to any registrar whose customer performs a check-command or Whois query for a string subject to Claims Plus. Registrars may then take further implementation steps to advise their customers, or use this data to better improve the customer experience. In addition, the Whois at the registry website will output a full Trademark Claims notice for any query of an unregistered name that is subject to Claims Plus. (Note: The ongoing availability of Claims Plus will be contingent on continued access to a Trademark Clearinghouse. The technical viability of some Claims Plus features will be affected by eventual Trademark Clearinghouse rules on database caching).

9.2 Domain Protected Marks List: The DPML is a rights protection mechanism to assist trademark holders in protecting their intellectual property against undesired registrations of strings containing their marks. The DPML prevents (blocks) registration of second level domains that contain a trademarked term (note: the standard for DPML is "contains"— the protected string must contain the trademarked term). DPML requests will be validated against the Trademark Clearinghouse and the process will be similar to registering a domain name so the process will not be onerous to trademark holders. An SLD subject to DPML will be protected at the second level across all Donuts TLDs (i.e. all TLDs for which this SLD is available for registration). Donuts may cooperate with other registries to extend DPML to TLDs that are not operated by Donuts. The cost of DPML to trademark owners is expected to be significantly less than the cost of actually registering a name.

10.0 ABUSIVE USE POLICIES AND TAKEDOWN PROCEDURES

In our response to Question #28, we describe our anti-abuse program, which is designed to address malware, phishing, spam, and other forms of abuse that may harm Internet users. This program is designed to actively discover, verify, and mitigate problems without infringing upon the rights of legitimate registrants. This program is designed for use in the open registration period. These procedures include the reporting of compromised websites⁄domains to registrars for cleanup by the registrants and their hosting providers. It also describes takedown procedures, and the timeframes and circumstances that apply for suspending domain names used improperly. Please see the response to Question #28 for full details.

We will institute a contractual obligation that proxy protection be stripped away if a domain is proven to be used for malicious purposes. For details, please see “Proxy⁄Privacy Service Policy to Curb Abuse” in the response to Question 28.

11.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO RIGHTS PROTECTION

We will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9. In rights protection matters, we will comply by establishing an adequate “firewall” between the operations of any registrar we establish and the operations of the registry. As the Code requires, we will not “directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services”. Here is a non-exhaustive list of specific steps we will take to accomplish this:

- We will evaluate and execute upon all rights protection tasks impartially, using the same criteria and procedures, regardless of a domain’s sponsoring registrar.
- Any registrar we establish or have established at the time of registry launch will not receive preferential access to any premium names, any auctions, etc. Registry personnel and any registrar personnel that we may employ in the future will be prohibited from participating as bidders in any auctions for Landrush names.
- Any registrar staff we may employ in the future will have access to data and records relating only to the applications and registrations made by any registrar we establish, and will not have special access to data related to the applications and registrations made by other registrars.
- If a compliance function is involved, the compliance staffer will be responsible to the registry only, and not to a registrar we own or are “affiliated” with. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that staffer will not have duties with the registrar business. The staffer will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry effectively and impartially, regardless of the consequences to the registrar.

12.0 ADDITIONAL PROTECTIONS

Due to the level of end-user trust potentially associated with this string Donuts will employ these additional four protections to minimize abuse:

1. For this string, to supplement the periodic audit documented above, a deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes;

2. Exclusion of registrars with a history of poor compliance;

3. Regular monitoring by the registry of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes; and

4. In addition to registry-based procedures, requirements that registrars have a 24⁄7⁄365 abuse contact, and remediation and takedown processes.

13.0. RESOURCING PLAN

Overall management of RPMs is the responsibility of Donuts' VP of Business Operations. Our back-end registry operator will perform the majority of operational work associated with RPMs, as required by our agreement with them. Donuts VP of Business Operations will supervise the activity of this vendor.

Resources applied to RPMs include:

1. Legal team
a. We will have at least one legal counsel who will be dedicated to the registry with previous experience in domain disputes and Sunrise periods and will oversee the compliance and support teams with regard to the legal issues related to Sunrise and RPM's
b. We have outside counsel with domain and rights protection experience that is available to us as necessary
2. Dispute Resolution Provider (DRP): The DRP will help formulate Sunrise Rules and Policy, Sunrise Dispute Resolution Policy. The DRP will also examine challenges, but the challenger will be required to pay DRP fees directly to the DRP.
3. Compliance Department and Tech Support: There will be three dedicated personnel assigned to these areas. This staff will oversee URS requests and abuse reports on an ongoing basis.
4. Programming and technical operations. There are four dedicated personnel assigned to these functions.
5. Project Manager: There will be one person to coordinate the technical needs of this group with the registry IT department.

13.0. ENDNOTES

1 "Regional" is understood to be a trans-national trademark registry, such as the European Union registry or the Benelux Office for Intellectual Property.

30(a). Security Policy: Summary of the security policy for the proposed registry

Q30a SV Char: 19960

1.0   INTRODUCTION

Our Information Security (IS) Program and associated IS Policy, Standards and

Procedures apply to all Applicant entities, employees, contractors, temps, systems, data, and processes. The Security Program is managed and maintained by the IS Team, supported by Executive Management and the Board of Directors.

Data and systems vary in sensitivity and criticality and do not unilaterally require the same control requirements. Our security policy classifies data and systems types and their applicable control requirements. All registry systems have the same data classification and are all managed to common security control framework. The data classification applied to all registry systems is our highest classification for confidentiality, availability and integrity, and the supporting control framework is consistent with the technical and operational requirements of a registry, and any supporting gTLD string, regardless of its nature or size. We have the experienced staff, robust system architecture and managed security controls to operate a registry and TLD of any size while providing reasonable assurance over the security, availability, and confidentiality of the systems supporting critical registry functions (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services).

This document describes the governance of our IS Program and the control frameworks our security program aligns to (section 1.0), Security Policy requirements (section 2.0); security assessments conducted (see section 3.0), our process for executive oversight and visibility of risks to ensure continuous improvement (section 4.0), and security commitments to registrants (section 5). Details regarding how these control requirements are implemented, security roles and responsibilities and resources supporting these efforts are included in Security Policy B response.

2.0. INFORMATION SECURITY PROGRAM

The IS Program for our registry is governed by an IS Policy aligned to the general clauses of ISO 27001 requirements for an Information Security Management System (ISMS) and follows the control objectives where appropriate, given the data type and resulting security requirements. (ISO 27001 certification for the registry is not planned, however, our DNS⁄DNSSEC solution is 27001 certified). The IS Program follows a Plan-Do-Check-Act (PDCA) model of continuous improvement to ensure that the security program grows in maturity and that we provide reasonable assurance to our shareholders and Board of Directors that our systems and data are secure.

The High Security Top Level Domain (HSTLD) control framework incorporates ISO 27002, the code of practice for implementing an ISO 27001 ISMS. Therefore, our security program is already closely aligned to the HSTLD control framework. Furthermore, we agree to abide by the HSTLD Principle 1 and criteria 1.1 - 1.3. (See specifics in Security Policy B response):

Registry systems will be in-scope for Sarbanes-Oxley (SOX) compliance and will follow the SOX control framework governing access control, account management, change management, software development life cycle (SDLC), and job monitoring of all systems. Registry systems will be tested frequently by the IS team for compliance and audited by our internal audit firm, Protiviti, and external audit firm, Price Waterhouse Coopers (PWC), for compliance.

2.1. SECURITY PROGRAM GOVERNANCE

Our Information Security Program is governed by IS Policy, supported by standards, and guided by procedures to ensure uniformed compliance to the program. Standards and associated procedures in support of the policy are shown in Attachment A, Figure 1. Security Program documents are updated annually or upon any system or environment change, new legal or regulatory requirements, and⁄or findings from risk assessments.

Any updates to security program are reviewed and approved by the Executive Vice President of IT, the General Counsel, and the EVP of HR before dissemination to all employees.

All employees are required to sign the IS Policy upon hire, upon any major changes, and⁄or annually. By signing the IS Policy, employees agree to abide by the supporting Standards and Procedures applicable to their job roles. To enable signing of the IS Policy, employees must pass a test to ensure competent understanding of the IS Policy and its key requirements.

3.0. INFORMATION SECURITY POLICY

3.1. INFORMATION ASSET CLASSIFICATION

The following data classification is applied to registry systems: High Business Impact (HBI): Business Confidential in accordance with the integrity, availability and confidentiality requirements of registry operations. All registry systems will follow Security Policy requirements for HBI systems regardless of the nature of the TLD string, financial materiality or size. HBI data if not properly secured, poses a high degree of risk to the registry and includes data pertaining to the registry’s adherence to legal, regulatory and compliance requirements, mergers and acquisitions (M&A), and confidential data inclusive of, but is not limited to: Personally Identifiable Information (PII) (credit card data, Social Security Numbers (SSN) and account numbers); materially important financial information (before public disclosure), and information which the Board of Directors (BoD)⁄Executive team deems to be a trade secret, which, if compromised, would cause grave harm to the execution of our business model.

HBI safeguards are designed, implemented and measured in alignment with confidentiality, integrity, availability and privacy requirements characterized by legal, regulatory and compliance obligations, or through directives issued by the BoD and Executive team. Where guidance is provided, such as the Payment Card Industry (PCI) Data Security Standard (DSS) Internal Audit Risk Control Matrices (RCMs), local, state and federal laws, and other applicable regulations, we put forth the appropriate level of effort and resources to meet those obligations. Where there is a lack of guidance or recommended safeguards, Risk Treatment Plans (RTP’s) are designed in alignment with our standard risk management practices.

Other data classifications for Medium Business Impact (MBI): Business Sensitive and Low Business Impact (LBI): Public do not apply to registry systems.

3.2. INFORMATION ASSET MANAGEMENT

All registry systems have a designated owner and⁄or custodian who ensure appropriate security classifications are implemented and maintained throughout the lifecycle of the asset and that a periodic review of that classification is conducted. The system owner is also responsible for approving access and the type of access granted. The IS team, in conjunction with Legal, is responsible for defining the legal, regulatory and compliance requirements for registry system and data.

3.3. INFORMATION ASSET HANDLING, STORAGE & DISPOSAL

Media and documents containing HBI data must adhere to their respective legal, regulatory and compliance requirements and follow the HBI Handling Standard and the retention requirements within the Document Retention Policy.

3.4. ACCESS CONTROL

User authentication is required to access our network and system resources. We follow a least-privileged role based access model. Users are only provided access to the systems, services or information they have specifically been authorized to use by the system owner based on their job role. Each user is uniquely identified by an ID associated only with that user. User IDs must be disabled promptly upon a user's termination, or job role change.

Visitors must sign-in at the front desk of any company office upon arrival and escorted by an employee at all times. Visitors must wear a badge while on-site and return the badge when signing out at the front desk. Dates and times of all visitors as well as the name of the employee escorting them must be tracked for audit purposes.

Individuals permitted to access registry systems and HBI information must follow the HBI Identity & Access Management Standard. Details of our access controls are described in Part B of Question 30 response including; technical specifications of access management through Active Directory, our ticketing system, physical access controls to systems and environmental conditions at the datacenter.

3.5. COMMUNICATIONS & OPERATIONAL SECURITY

3.5.1. MALICIOUS CODE

Controls shall be implemented to protect against malicious code including but not limited to:
- Identification of vulnerabilities and applicable remediation activities, such as patching, operating system & software upgrades and⁄or remediation of web application code vulnerabilities.
- File-integrity monitoring shall be used, maintained and updated appropriately.
- An Intrusion Detection Solution (IDS) must be implemented on all HBI systems, maintained & updated continuously.
- Anti-virus (AV) software must be installed on HBI classified web & application systems and systems that provide access to HBI systems. AV software and virus definitions are updated on a regular basis and logs are retained for no less than one year.

3.5.2. THREAT ANALYSIS & VULNERABILITY MANAGEMENT

On a regular basis, IS personnel must review newly identified vulnerability advisories from trusted organizations such as the Center for Internet Security, Microsoft, SANS Institute, SecurityFocus, and the CERT at Carnegie-Mellon University. Exposure to such vulnerabilities must be evaluated in a timely manner and appropriate measures taken to communicate vulnerabilities to the system owners, and remediate as required by the Vulnerability Management Standard. Internal and external network vulnerability scans, application & network layer penetration testing must be performed by qualified internal resource or an external third party at least quarterly or upon any significant network change. Web application vulnerability scanning is to be performed on a continual basis for our primary web properties applicable to their release cycles.

3.5.3. CHANGE CONTROL

Changes to HBI systems including operating system upgrades, computing hardware, networks and applications must follow the Change Control Standard and procedures described in Security Policy question 30b.

3.5.4. BACKUP & RESTORATION

Data critical to our operations shall be backed up according to our Backup and Restoration Standard. Specifics regarding Backup and Restoration requirements for registry systems are included in questions 37 & 38.

3.6. NETWORK CONTROLS

- Appropriate controls must be established for ensuring the network is operated consistently and as planned over its entire lifecycle.
- Network systems must be synchronized with an agreed upon time source to ensure that all logs correctly reflect the same accurate time.
- Networked services will be managed in a manner that ensures connected users or services do not compromise the security of the other applications or services as required in the HBI Network Configuration Standard. Additional details are included in Question 32: Architecture response.

3.7. DISASTER RECOVERY & BUSINESS CONTINUITY

The SVP of IT has responsibility for the management of disaster recovery and business continuity. Redundancy and fault-tolerance shall be built into systems whenever possible to minimize outages caused by hardware failures. Risk assessments shall be completed to identify events that may cause an interruption and the probability that an event may occur. Details regarding our registry continuity plan are included in our Question 39 response.

3.8 SOFTWARE DEVELOPMENT LIFECYCLE

Advance planning and preparation is required to ensure new or modified systems have adequate security, capacity and resources to meet present and future requirements. Criteria for new information systems or upgrades must be established and acceptance testing carried out to ensure that the system performs as expected. Registry systems must follow the HBI Software Development Lifecycle (SDLC) Standard.

3.9. SECURITY MONITORING

Audit logs that record user activities, system errors or faults, exceptions and security events shall be produced and retained according to legal, regulatory, and compliance requirements. Log files must be protected from unauthorized access or manipulation. IS is responsible for monitoring activity and access to HBI systems through regular log reviews.

3.10. INVESTIGATION & INCIDENT MANAGEMENT RESPONSE

Potential security incidents must be immediately reported to the IS Team, EVP of IT, the Legal Department and⁄or the Incident Response email alias. The Incident Response Team (IRT) is required to investigate: any real or suspected event that could impact the security of our network or computer systems; impose significant legal liabilities or financial loss, loss of proprietary data⁄trade secret, and⁄or harm to our goodwill. The Director of IS is responsible for the organization and maintenance of the IRT that provides accelerated problem notification, damage control, investigation and incident response services in the event of security incidents. Investigation and response processes follow the requirements of the Investigation and Incident Management Standard and supporting Incident Response Procedure (see Question 30b for details).

3.11. LEGAL & REGULATORY COMPLIANCE

All relevant legal, regulatory and contractual requirements are defined, documented and maintained within the IS Policy. Critical records are protected from loss, destruction and falsification, in accordance with legal, contractual and business requirements as described in our Document Retention Policy. Compliance programs implemented that are applicable to Registry Services include:

- Sarbanes Oxley (SOX): All employees managing and accessing SOX systems and/or data are required to follow SOX compliance controls.
- Data Privacy and Disclosure of Personally Identifiable Information (PII): data protection and privacy shall be ensured as required by legal and regulatory requirements, which may include state breach and disclosure laws, US and EU Safe Harbor compliance directives.

Other compliance programs implemented but not applicable to Registry systems include the Payment Card Industry (PCI) Data Security Standard (DSS), Office of Foreign Assets Control (OFAC) requirements, Copyright Infringement & DMCA.

4.0. SECURITY ASSESSMENTS

Our IS team conducts frequent security assessments to analyze threats, vulnerabilities and risks associated with our systems and data. Additionally, we contract with several third parties to conduct independent security posture assessments as described below. Details of these assessments are provided in our Security Policy B response.

4.1. THIRD PARTY SECURITY ASSESSMENTS

We outsource the following third party security assessments (scope, vendor, frequency and remediation requirements of any issues found are detailed in our Security Policy B response); Web Application Security Vulnerability testing, quarterly PCI ASV scans, Sarbanes-Oxley (SOX) control design and operating effectiveness testing and Network and System Security Analysis.

4.2. INTERNAL SECURITY ASSESSMENTS

The IS team conducts routine and continual internal testing (scope, frequency, and remediation requirements of any issues found are detailed in our Security Policy B response) including; web application security vulnerability testing, external and internal vulnerability scanning, system and network infrastructure penetration testing, access control appropriateness reviews, wireless access point discovery, network security device configuration analysis and an annual comprehensive enterprise risk analysis.

5.0. EXECUTIVE OVERSIGHT & CONTINUOUS IMPROVEMENT

In addition to the responsibility for Information Security residing within the IS team and SVP of IT, risk treatment decisions are also the responsibility of the executive of the business unit responsible for the risk. Any risk with potential to impact the business financially or legally in a material way is overseen by the Incident Response Management team and/or the Audit Committee. See Figure 2 in Attachment A. The Incident Response Management Team or Audit Committee will provide assistance with management action plans and remediation.

5.1. GOVERNANCE RISK & COMPLIANCE

We have deployed RSA’s Archer Enterprise Governance Risk and Compliance (eGRC) Tool to provide an independent benchmarking of risk, compliance and security metrics, assist with executive risk reporting and reduce risk treatment decision making time, enforcing continuous improvement. The eGRC provides automated reporting of registry systems compliance with the security program as a whole, SOX Compliance, and our Vulnerability Management Standard. The eGRC dashboard continuously monitors risks and threats (through automated feeds from our vulnerability testing tools and third party data feeds such as Microsoft, CERT, WhiteHat, etc.) that are actionable. See Attachment A for more details on the GRC solutions deployed.

6.0. SECURITY COMMITMENTS TO REGISTRANTS

We operate all registry systems in a highly secured environment with appropriate controls for protecting HBI data and ensuring all systems remain confidential, have integrity, and are highly available. Registrants can assume that:

1. We safeguard the confidentiality, integrity and availability of registrant data through access control and change management:
   - Access to data is restricted to personnel based on job role and requires 2 factors of authentication.
   - All system changes follow SOX-compliant controls and adequate testing is performed to ensure production pushes are stable and secure.
2. The network and systems are deployed in high availability with a redundant hot datacenter to ensure maximum availability.
3. Systems are continually assessed for threats and vulnerabilities and remediated as required by the Vulnerability Management Standard to ensure protection from external malicious acts.
   - We conduct continual testing for web code security vulnerabilities (cross-site scripting, SQL Injection, etc.) during the development cycle and in production.
4. All potential security incidents are investigated and remediated as required by our Incident Investigation & Response Standard, any resulting problems are managed to prevent any recurrence throughout the registry.

We believe the security measures detailed in this application are commensurate with the nature of the TLD string being applied for. This string might be considered by some to have public trust implications (as discussed in Guidebook Q30), accordingly, the following additional security measures will be implemented to protect consumers using this TLD including, but not limited to:

1. Periodic audit of Whois data for accuracy.
2. Deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes.
3. Regular monitoring of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes.
4. A new Domain Protected Marks List (DPML) product for trademark protection;
5. A new Claims Plus product for trademark protection;
6. Terms of use that prohibit illegal or abusive activity;
7. Limitations on domain proxy and privacy service;
8. Published policies and procedures that define abusive activity
9. Require that registrars have a 24/7/365 abuse contact and a remediation / takedown processes.
10. Exclusion of registrars with a history of poor compliance.
11. Proper resourcing for all of the functions above.

7.0 RESPONSIBILITY OF INFORMATION SECURITY
See Question B Response Section 10.

© Internet Corporation For Assigned Names and Numbers.

Annex B - Exhibit 2

Applicant’s gTLD Portfolio

donuts

ACADEMY
ACCOUNTANTS
AGENCY
APARTMENTS
APP
ARCHITECT
ART
ASSOCIATES
ATTORNEY
AUCTION
AUDIO
AUTO
BABY
BAND
BARGAINS
BASEBALL
BASKETBALL
BEAUTY
BET
BIKE
BINGO
BLOG
BOATS
BOOK
BOUTIQUE
BROADWAY
BROKER
BUILDERS
BUSINESS
BUY
CAB
CAFÉ
CAMERA
CAMP
CAPITAL
CARDS
CARE
CAREERS
CARS
CASA
CASH
CASINO
CATERING
CENTER
CHARITY
CHAT
CHEAP
CHURCH
CITY
CLAIMS
CLEANING
CLINIC
CLOTHING
CLOUD
CLUB
COACH
CODES
COFFEE
COLLEGE
COMMUNITY
COMPANY
COMPUTER
CONDOS
CONSTRUCTION
CONSULTING
CONTRACTORS
COOL
CORP
COUPONS
CPA
CREDIT
CREDITCARD
CRICKET
CRUISES
DATA
DATING
DEALS
DEGREE
DELIVERY
DENTAL
DENTIST
DESIGN
DIAMONDS
DIET
DIGITAL
DIRECT
DIRECTORY
DISCOUNT
DOCTOR
DOG
DOMAINS
ECO
EDUCATION
EMAIL
ENERGY
ENGINEERING
ENTERPRISES
EQUIPMENT
ESTATE
EVENTS
EXCHANGE
EXPERT
EXPOSED
EXPRESS
FAIL
FAMILY
FAN
FARM
FASHION
FILM
FINANCE
FINANCIAL
FISH
FITNESS
FLIGHTS
FLORIST
FLOWERS

FOOD
FOOTBALL
FORSALE
FORUM
FOUNDATION
FREE
FUND
FURNITURE
FUTBOL
FYI
GALLERY
GAMES
GARDEN
GIFTS
GLASS
GLOBAL
GMBH
GOLD
GOLF
GRAPHICS
GRATIS
GRIPE
GROUP
GUIDE
GURU
HAUS
HEALTH
HEALTHCARE
HELP
HOCKEY
HOLDINGS
HOLIDAY
HOME
HOSPITAL
HOSTING
HOT
HOTEL
HOUSE
IMMO
INC
INDUSTRIES
INSTITUTE
INSURANCE
INSURE
INTERNATIONAL
INVESTMENTS
JEWELRY
JUEGOS
KITCHEN
LAND
LAW
LAWYER
LEASE
LEGAL
LIFE
LIGHTING
LIMITED
LIMO
LIVE
LIVING
LLC
LOANS
LOVE
LTD
LUXURY
MAIL
MAISON
MANAGEMENT
MARKET
MARKETING
MBA
MEDIA
MEDICAL
MEMORIAL
MOBILE
MONEY
MORTGAGE
MOVIE
MUSIC
NETWORK
NEWS
NOW
ONLINE
PARTNERS
PARTS
PETS
PHONE
PHOTOGRAPHY
PHOTOS
PICTURES
PIZZA
PLACE
PLUMBING
PLUS
POKER
PRODUCTIONS
PROPERTIES
PROPERTY
RACING
RADIO
REALESTATE
REALTY
RECIPES
RED
REISEN
RENT
RENTALS
REPAIR
REPORT
RESTAURANT
REVIEWS
ROCKS
RUGBY
RUN
SALE
SALON
SARL
SCHOOL
SCHULE
SEARCH
SECURITY
SERVICES
SHOES
SHOP
SHOPPING
SHOW
SINGLES
SITE
SKI
SOCCER
SOFTWARE
SOLAR
SOLUTIONS
SPA
SPORTS
STORAGE
STORE
STUDIO

STYLE
SUCKS
SUPPLIES
SUPPLY
SUPPORT
SURGERY
SYSTEMS
TAX
TAXI
TEAM
TECH
TECHNOLOGY
TENNIS
THEATER
TICKETS
TIENDA
TIPS
TIRES
TODAY
TOOLS
TOURS
TOWN
TOYS
TRADING
TRAINING
TUBE
UNIVERSITY
VACATIONS
VENTURES
VET
VIAJES
VIDEO
VILLAS
VIN
VIP
VISION
VOTE
VOYAGE
WATCH
WEB
WEBSITE
WEDDING
WINE
WORKS
WORLD
WTF
YOGA
ZONE

游戏	GAMES
商店	SHOP or STORE
娱乐	ENTERTAINMENT
企业	ENTERPRISE

Annex C

Letter from ICANN Independent Objector

Independent Objector

Home

Introducing the Independent Objector

ICANN Applicant Guidebook for the New gTLD Program

Limited Public Interests Objections

Community Objections

The Dispute Resolution Process

The Independent Objector's Comments on Controversial Applications

The Issue of "Closed Generic" gTLDs

News

Contact

Contact

Pr. Alain Pellet
Independent Objector

Julien Boissise
Legal Assistant to the Independent Objector

Email:
Contact@Independent-Objector-newgtlds.org

You can also use our
Contact Form.

The Issue of "Closed Generic" gTLDs Applications - The Views of the Independent Objector

Description of the issue

1. ICANN has recently opened a 30-day public comments period to address the issue of “closed generic” gTLDs. ICANN seeks comments from interested stakeholders in order to explore potential new alternatives and provisions addressing the issue.
2. As the Independent Objector, I have faced the issue of “closed generic” gTLDs from the very beginning of my review of applications. Notably, several persons and entities reported directly to me their concerns on this issue and urged me to file objections against the concerned applications. I have decided not to do so on this sole ground. As I am acting on behalf of the public who use the global Internet and committed to full transparency, I deem it necessary to briefly explain my position in this respect.
3. In my view, a “generic term” is a word associated to goods, service, activities or market sectors, which is widely used by people and commonly understood as referring to the good, service, activity or market sector in question. It is supposedly not directly associated to a brand or trademark. However, sometimes trademarks or brands become generic terms, such as “Aspirin”.
4. I note that the core question is whether applicants, generally being companies and corporate entities, can have the benefit of a new gTLD string for their own use, notwithstanding the general use of the term by the public.
5. According to the new gTLDs Program Committee of the ICANN Board of Directors and its resolution of February 2, 2013, it is understood that “members of the community term a ‘closed generic’ TLD as a TLD string that is a generic term and is proposed to be operated by a participant exclusively for its own benefit”. Where the new gTLDs “program's goals include enhancing competition and consumer choice, and enabling the benefits of innovation via the introduction of new gTLDs”, opponents to applications for “closed generic” gTLDs argue that it would have a negative impact on competition and consumer choice.

The Independent Objector’s Mission

1. On this issue, it is important to insist on the core essence of the IO’s functions and his “limited powers” as described in the Applicant Guidebook, which constitutes the basis for his mandate under the new gTLDs Dispute Resolution Process.
2. The IO is only entitled to lodge objections on the limited public interest and community grounds. For both grounds for objection, he acts in complete independence, and solely in the best interests of the public who use the global

Internet.

3. In line with this public interest mission, the IO is only allowed to file objections when applications have been commented in the public sphere. He can only lodge an objection if no one else files previously an objection on the same ground, which implies that he is acting as a “safety net”.
4. When reviewing the applications, I have paid great attention to the related public comments, some of which addressed the issue of “closed generic” gTLDs.
5. While the present comment aims at explaining the reasons why I consider that the issue of “closed generic” gTLDs does not fall within the scope of my limited functions, it should be noted that the hereunder remarks are general; each application is reviewed separately and has specificities which could justify an objection from the IO for other reasons. It is also not the mission of the IO to express his personal position on the substance of the issue, nor to make suggestions and proposals to ICANN.
6. However, I acknowledge the importance of the problem. The question of the openness of new gTLDs is crucial, particularly when it comes to terms that could be profitable to a large part of the public, and this is undoubtedly the case concerning gTLDs strings such as “.search”, “.book”, “.beauty”, “.insurance”, “.blog”, “.shop”, “.music”, “.jewerly”, “.app” or “.cloud”, to mention the most commented ones.

Limited Public Interest Objections

1. In case of a limited public interest objection, the essential criterion is not to determine whether or not the application is contrary to the multiple potential interests of the public who use the global Internet. It is not the mission of the IO to protect personal or commercial interests of individual Internet users. This particular objection ground aims at ensuring that no applied-for gTLD string and its intended use is contrary to fundamental norms of public order and morality that are recognized under international law.
2. For instance, a limited public interests objection could be triggered in case an application promote unlawful activities or international crimes, such as child pornography, sale of counterfeit medicines, slavery, torture or genocide; in case it endangers international public order or again in case it is obviously against moral values that have been transcribed in international norms.
3. In its letter dated 31 January 2013, Microsoft argued that applied-for “generic closed” gTLDs strings “threaten the openness and freedom of the Internet and could have harmful consequences for Internet users worldwide”.
4. On the issue of the openness and freedom of the Internet, which is the main argument used by most opponents to “generic closed” gTLDs on the ground of the protection of the public interest, I acknowledge that there are fundamental principles of international law which should be protected. This is notably the case of the principle of freedom of expression, which is given a broad interpretation in international law as it encompasses the freedom of speech, opinion, expression and access to information. This freedom applies to the Internet as recalled by the United Nations Educational Scientific and Cultural Organization (UNESCO), which “recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge and opens up new opportunities for expression and participation. UNESCO assumes its responsibility of promoting freedom of expression on Internet and has integrated it to its regular program. The principle of freedom of expression must apply not only to traditional media but also to the Internet and all types of emerging media platforms which will definitely contribute to development, democracy and dialogue."

5. I also note that the issue of the openness of the Internet was discussed recently at the international level. The United Nations Human Rights Council requested the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, to further explore the issue. However, his reports do not, either directly or indirectly, address the issue of “closed gTLDs”, or more generally of the management of the DNS, and refer to “the advantages and challenges of new information and communications technologies, including the Internet and mobile technologies, for the exercise of the right to freedom of opinion and expression, including the right to seek, receive and impart information and the relevance of a wide diversity of sources, as well as access to the information society for all”. The Special Rapporteur’s reports notably address the issues of restrictions of content on the Internet, the access to the Internet and the necessary infrastructures, and general principles on the right to freedom of opinion and expression and the Internet.
6. However, while I recognize that certain questions raised by the openness of the Internet should be in line with fundamental principles of public order and morality recognized under international law,I also note that these principles are hardly relevant for the specific issue of “closed generic” gTLDs. Indeed, I have strong doubts that the question of closed gTLDs is related to the problematic of public order: the issue might be linked to commercial interests, it is not directly linked with the freedom of expression.
7. Therefore, whether applicants can beneficiate of a new gTLD string for their own use, notwithstanding the general use of the term by the public, does not seem to be an issue that I could invoke to justify an objection on this ground. Therefore, a limited public interest objection would not be warranted for those applications, at least on the ground of the openness of the access to a gTLD.

Community Objections

1. For every application I review, I also assess whether a community objection could be warranted. I examine whether there is a 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 communities in question must be strongly associated with the applied-for gTLD string in the application that is the subject of the objection.
2. I base my evaluation on four eliminatory tests, which are set out in the Applicant Guidebook in order to guide the Expert panels for the evaluation of community objections. The gTLD string must explicitly or implicitly target a specific community. The targeted community must be clearly delineated. I verify if there is a substantial opposition to the gTLD application from a significant portion of the community. Finally, I assess whether the application for the gTLD string creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted.
3. As for the community test, (the IO determines if the community invoked is a clearly delineated community), the notion of “community” is wide and broad, and is not precisely defined by ICANN’s Applicant Guidebook for the new gTLDs program. It can include a community of interests, as well as a particular ethnical, religious, linguistic or similar community. Moreover, communities can also be classified in sub-communities (i.e. the Jewish community in New York or the Italian community on Facebook). However, beyond the diversity of communities, there are common definitional elements and a community can be defined as a group of individuals who have something in common (which can include their nationality or place of residence – i.e. the French, South-East Asian or Brazilian community – or a common

characteristic – i.e. the disability community), or share common values, interests or goals (i.e. the health or legal community). For the purpose of the IO evaluation, it is clear that what matters is that the community invoked can be clearly delineated, enjoys a certain level of public recognition and encompasses a certain number of people and/or entities.

4. In view of the broad elements of definition mentioned above, and more pertinently in view of the very nature of a "generic term", it is unlikely that these applications will pass this community test. Of course for a community objection, each application has to be reviewed separately. However, as a general remark and because I have reviewed all applications, it is difficult in these cases to prove the existence of a clearly delineated community. By definition, a "generic term" is a term which is used by a significant number of people, who do not necessarily share similar goals, values or interests. A specific community should distinguish itself from others, precisely by its characteristics or specificities. It cannot be the case for a "generic term" which, by definition, goes beyond specificities as it is used by very different persons. Therefore, while I fully understand the concerns expressed on behalf of the public who use the Internet, the latter cannot be considered as a clearly delineated community. When criteria for this test are not met on this basis, a community objection is not warranted.
5. I have however reviewed all the applications in order to make sure that in each case, no clearly delineated community, generally referring to a particular industry, was substantially opposed to the string and that their interests were not threatened. As a general observation, I have to note that in most cases, such a delineated community does not exist.
6. Taking ".book" as an example, the "book industry" and a hypothetical "book community" would encompass a large variety of stakeholders, who do not always share similar primary interests. Thus, it would include authors, publishers, libraries, retailers, readers, etc… In a more inclusive way, we could also include international organizations working, *inter alia*, for the promotion of culture such as the UNESCO. Therefore, these different stakeholders are difficult to be delineated as a single community since they are of very different nature. Some have the promotion of literature as their primary aim but for many others it is one objective among many others. It is therefore quite doubtful that they represent a clearly delineated community within the meaning of the Applicant Guidebook.
7. Therefore, I note that, in general, for the issue of "closed generic" gTLDs and my possibility to object as the IO on the community ground, it is unlikely that the applications concerned meet the four tests. However, it is important to note that for an assessment on the community ground, each application has to be reviewed separately. The present comment only affirms that a community objection cannot be lodged on behalf of the public who uses the Internet as a whole, which cannot be considered as a clearly delineated community.
8. Moreover, as for my possibility to object on the community ground, it is my clearly explained public policy not to make an objection when a single established institution representing and associated with the community having an interest in an objection can lodge such an objection directly. This does not exclude that I could deem it nevertheless appropriate to file a community objection in exceptional circumstances, in particular if the established institution representing and associated with the community has compelling reasons not to do so, or if several institutions could represent a single community and are in the same interest so that an application could raise issues of priority, or in respect to the modalities of the objection. The objections I have just filed are based on such assessments.

Attachment 3

[IO Reply]

International Chamber of Commerce
The world business organization

International Centre for Expertise   Centre international d'expertise

NEW GENERIC TOP-LEVEL DOMAIN NAMES (“gTLD”) DISPUTE RESOLUTION PROCEDURE

ADDITIONAL WRITTEN STATEMENT

Filed by the Independent Objector

Community Objection

Disputed gTLD

gTLD Objector objects to

Name	.Charity (Application ID: 1-1384-49318)
ICC Case No.	EXP/395/ICANN/12

EXPERT PANEL

Name	Mr. Tim Portwood
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

© International Chamber of Commerce (ICC) December 2012. All rights reserved. No part of this document may be reproduced or copied in any form or by any means, or translated, without the prior permission in writing of ICC.

Identification of the Parties, their Representatives and related entities

Objector

Name	Prof. Alain Pellet, Independent Objector
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Objector's Representative(s)

Name	Ms Héloïse Bajer-Pellet
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Daniel Müller
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Phon van den Biesen
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Name	Mr. Sam Wordsworth, QC
Contact	Contact Information Redacted
Address	
City, Country	
Telephone	
Email	

Applicant

Name	Corn Lake, LLC
Contact person	Daniel Schindler, Jon Nevett
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Applicant's Representative(s)

Name	The IP & Technology Legal Group, P.C. dba New gTLD Disputes http://www.newgtlddisputes.com
Contact person	John M. Genga, Don C. Moody
Address	Contact Information Redacted
City, Country	

Telephone	Contact Information Redacted
Email	

Applicant's Contact Address

Name	The IP & Technology Legal Group, P.C. dba New gTLD Disputes http://www.newgtlddisputes.com
Contact person	John M. Genga, Don C. Moody
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Procedure

On 12 March 2013, the Independent Objector filed electronically a Community objection to the Application of Corn Lake LLC, for the gTLD string .Charity (Application ID: 1-1384-49318). Electronic copies of the objection were transmitted to the Applicant and to ICANN on 13 March 2013.

On 28 March 2013, the DRSP informed the Independent Objector that it "has conducted the administrative review of the Objection in the above-referenced matter (Article 9 of the Procedure)" and that "the Objection is in compliance with Articles 5 – 8 of the Procedure and with the Rules."

On 7 May 2013, the DRSP further informed the Parties that ICANN had published its Dispute Announcement pursuant to Article 10(a) of the Procedure on 12 April 2013. It invited the Applicant to file a Response within 30 days of the transmission of this invitation (Article 11(b) of the Procedure).

On 6 June 2013, the Applicant filed electronically its Response to the Objection with Annexes. Electronic copies were transmitted to the Independent Objector and its representatives, as well as to ICANN.

On 10 July 2013, the DRSP informed the Parties that the Chairman of the Standing Committee had appointed Mr. Tim Portwood as the Expert in the case and invited both Parties to make the required advance payment of costs for the Panel to be fully constituted. On 2 August 2013, the DRSP further informed the Parties of the receipt of the necessary advance payment and transferred the case file to the Expert Panel.

By e-mail of 2 August 2013, the Independent Objector requested permission to file an additional written statement in order to address new issues which have been raised by Applicant's response. This request was granted by the Expert Panel. The Expert Panel fixed the time limit for the Independent Objector's additional written statement on 24 August 2013.

The present Additional Written Statement is filed accordingly.

Observations on the Response submitted by the Applicant

1. Applicant's Response to the Community objection filed by the Independent Objector (IO) concerning its Application for the .Charity gTLD raises a number of issues on which the IO wishes to provide some further clarifications in order to assist the Expert Panel in its task and to refine the standards fixed in the Applicant's Guidebook (hereafter the "Guidebook").

1. IO's impartiality and independence

2. The IO has filed this objection (and all others objections) in accordance with Article 3.2.5 of the Guidebook stating that "the IO must be and remain independent". So he is. Contrary to the regrettable suggestions made in the Response (pp. 5 and 13), the IO does not act in accordance with what he "himself might prefer" nor with "self-interest". He is acting exclusively in the best interests of the public who use the global Internet.

2. The Standing of the Independent Objector is not Limited as Suggested by the Applicant

3. The Applicant misconceives the requirements concerning the IO's standing to file a Community objection. Despite the clear wording of the relevant provisions of the Guidebook, and in particular its Article 3.2.5, the Applicant submits that the IO has to prove that he is acting "on behalf of a 'clearly delineated community'" and that the applied for string is strongly associated with the named community (Response, p. 6).

4. The text of the Guidebook is unambiguous on the role and the function of the IO. Contrary to Applicant's position, the IO does not represent a community even in the event of a Community objection. Article 3.2.5 points to this fact, underlining that "[t]he 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". For this reason it is manifestly incorrect to test the IO's standing by reference to the existence or representation of a clearly delineated community. This test is part of the substantive standards elaborated by ICANN and enshrined in the Guidebook (Article 3.5.4), and nothing suggests that it separately constitutes an additional standing requirement for the IO.

5. To the contrary, even if other objectors might be required to demonstrate not only their specific link with the community[1], but also its clearly delineated character, these

[1] This is indeed suggested by the *travaux*: "The objector must provide verifiable evidence that it is an established institution of the community" (see Implementation Guideline P, Final Report on the

requirements are expressly disposed of as far as the IO is concerned. Article 3.2.5 of the Guidebook states in terms: “The IO *is granted standing* to file objections on these enumerated grounds [i.e., Limited Public Interest objections and Community objections], notwithstanding the regular standing requirements for such objections” (emphasis added). The IO therefore has *ipso facto* standing in the sense of Article 3.2.2 of the Guidebook and his objection must be considered on its merits. The only limitation put to the wide discretion of the IO is embodied in the last paragraph of Article 3.2.5: “In light of the public interest goal noted above, the IO shall not object to an application unless at least one comment in opposition to the application is made in the public sphere.” This has been underlined by the IO[2]. This condition is fulfilled in the present case, as has been shown by the IO (Objection, p. 5) and as the Applicant itself recognizes (even if it contests the comments being in opposition to its Application) (Response, pp. 9-10).

6. For these reasons, Applicant’s request for the Panel to dismiss the Objection on standing is ill-founded.

3. Applicant’s Misconceived Understanding of the Community Objection and the Underlying Principles

7. The Applicant seems to imply in its response that, under the Community objection ground, a community could prevent the use of a string for its own purposes. It contends: “The notion of a charity ‘community,’ which would allow a single party such as the Objector to prevent the use of a dictionary term to the exclusion of all others, defies reason. Such a scheme contravenes the open nature of the Internet and the intent of ICANN in adopting the new gTLD program.” (Response, p. 6) This is misconceived. The Guidebook does not require that any and every gTLD string which targets a community must necessarily be applied for by a representative of the community (even if it gives some preference to such community based applications against applications which have no support from the community; see Article 4.2.3). A string targeting a community is not as such reserved by or for this community to the exclusion of all others. However, the operation of such a new gTLD should not cause material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted. If this is not the case, there is no reason not to allow a technically sound application to proceed.

Introduction of New Generic Top-Level Domains, 8 August 2007, http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm).

[2] See, e.g., http://www.independent-objector-newgtlds.org/english-version/the-issue-of-closed-generic-gtlds/.

8. The problem is therefore not so much whether the Applicant could apply for a string like .Charity, but rather if it can use and operate this gTLD in the way it describes in its Application. It is therefore irrelevant whether the Applicant wants to reach a specific community, or whether it does or does not intend to reserve its gTLD for a specific community. The Guidebook clearly points out: “All applicants should understand that a formal 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.” (Article 1.2.3.2). The Applicant and Donuts, its ultimate parent, were entirely aware of this possibility. Its own understanding and policy of what the Internet should look like and its comparison of existing domain names within the gTLD .com, cannot prevail over the safeguards incorporated into the Guidebook. Even if Donuts has submitted a great number of applications under the gTLD Program, and has made large investments in application fees, it is not entitled to frame or to change the policy of the program as best fits its own philosophy and business model (see Response, Annex B, paras. 4-6).

9. Indeed, the IO has assumed the responsibility and duty to review all applications for New gTLDs and to apply the rules enshrined in the Guidebook in order to determine whether to object. It has always been plain that a possible consequence of IO submitting an objection is that an application may be rejected. The rejection of an application following a successful objection is not an unwarranted violation of the fundamental rights of freedom of expression. Instead, any such rejection flows from the application of the dispute resolution system instituted alongside the New TLD programme.

4. The Interpretation of the Community and the Targeting Tests

10. The Applicant contends that the IO has failed to evidence a clearly delineated community as required by Article 3.5.4 of the Guidebook (Response, p. 7). Article 3.5.4 of the Guidebook lists factors a panel could balance to determine whether a clearly delineated community exists. However, that list is only guidance and is not exhaustive or exclusive.

11. Applicant’s interpretation and application of the Community test and the Targeting test (see in particular in Article 3.5.4) ignore the wording and the object and purpose of these standards. Assuming incorrectly that the IO has to demonstrate the existence of a “ ‘clearly delineated’ community” as part of the standing requirements (see above), the Applicant asserts that the IO “must overcome a more stringent test on the merits than he need do for standing” (Response, p. 7). For the Applicant, such a “more stringent test” consists of showing that the string itself describes a clearly delineated community (Response, pp. 6 and 8).

12. This assertion is unsupported and runs counter to the separate nature of the Community test, which is aimed at proving that the "community expressing opposition can be regarded as a clearly delineated community" (Guidebook, Article 3.5.4), and the Targeting test, according to which "[t]he objector must prove a strong association between the applied-for gTLD string and the community represented by the objector." (*ibid.*) If the? Applicant's "more stringent test" were to prevail, there would indeed be little room for the Targeting test as described in the Guidebook: because if the applied for gTLD string needs to describe the community, the string would necessarily imply a "strong association", if not more, between the string and the community. According to Applicant's own standard of *ut res magis valeat quam pereat* (Response, p. 7), both tests have to be given an effective meaning, rather than being useless or redundant.

13. Moreover, none of the illustrative elements listed in the Guidebook with respect to the Community test implies that the applied for string has to "describe" a community (whatever this actually means). The objector has to demonstrate that the community which expresses opposition to an application is a "clearly delineated community" rather than a simple group of people or entities. It is therefore irrelevant, so far as this first test is concerned, if the string actually "describes" the community or not. Even if Applicant's assertion – that "charity" is nothing else but a subject of interest to everybody and has a broad meaning (Response, pp. 6 and 8) – were true this does not in itself imply that there cannot be a "charity community" satisfying the test of a delineated community in the sense of the Guidebook. Only the characteristics of the community have to be taken into account for this assessment, not the meaning of the string "charity".

14. In any event, although one use of the word "charity" may be to describe the general matter of acting charitably, another and most obvious use of the word is as a noun used to describe charities and charitable organisations. These in turn are a recognizable "community" with specific values and goals and particular needs. The IO does not contend, as the Response at p. 7 wrongly suggests, that the community is "millions of persons and organizations worldwide…". That describes the community targeted by the Applicant but, as discussed below, it is not the relevant community identified by the IO. Further, the IO does not suggest that the word "charity" has just one meaning. The IO merely reiterates that the meaning of the gTLD string is not the relevant test for ascertaining whether there is a clearly delineated community.

15. The crucial element for the Community test is whether "the group of individuals or entities can be clearly delineated from others, and whether members of the 'community [are] delineated from Internet users in general'" (Objection, para. 18 (reference omitted)). There is no indication in the Guidebook, but also no limitation, concerning the factors which can be

used to delineate the community *vis-à-vis* others. It is, however, clear that the community needs to be something more than a mere group of peoples or entities.

16. The IO has demonstrated that the "charity community" does satisfy the Community test as described in the Guidebook (Objection, paras. 15 – 21). Even if it is not entirely homogenous and institutionalised but instead encompasses several stakeholders, it is nonetheless a recognizable community which can be delineated through distinctive criteria that evidence the values and characteristics shared by the charity community.

17. The IO's conclusion is in effect confirmed in the Advice contained in the GAC's Beijing Communiqué, dated 11 April 2013[3], which has not been disputed by the Applicant in its Response to the Panel (despite Donuts' very strong concerns expressed in the month before the filing of the Response in the present case[4]). It is indeed striking that the GAC has not only included .Charity in its list of sensitive strings necessitating particular safeguard measures[5], but has also pointed to the fact that strings in the charity segment, including .Charity, are part of those strings "associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions."[6] It is also underlined that .Charity is one of the strings that are "linked to *regulated or professional sectors* [that] should operate in a way that is consistent with applicable laws" as they are "likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm".[7] The GAC has therefore indicated that the charity community can be clearly delineated through the clear and/or regulated entry requirements and credentials which should be verified by registrars at registration and throughout the operation of a registered domain[8].

18. Applicant's interpretation of the Targeting test is also flawed. Applicant largely focuses on the very inclusive group it wants to be able to register domain names within the .Charity gTLD, which in the understanding of Applicant means everybody. It is not the Application that has to target a community, but the string in itself. The intended use of the string by the Applicant constitutes only one element in order to assess the "strong association" between the string and a community. But it is not the only one, and certainly not the most reliable one. What matters much more is whether the general public is likely to

[3] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf (Annex 1).

[4] http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf.

[5] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf, Annex I, Category 1, pp. 8-9 (Annex 1).

[6] *Ibid.*, p. 10 (Annex 1).

[7] *Ibid.*, p. 8 (Annex 1) (emphasis added)

[8] *Ibid.*, p. 10 (point 6) (Annex 1).

make a strong association between the string and the defined community, and here what counts is not specifically whether the string expressly describes a community as such, but whether the string is sufficiently linked with the community. Applicant's arguments concerning the lack of targeting are therefore inconclusive. This is in particular true with respect to the dictionary definitions it uses to show a broader understanding of the string "charity" (Response, p. 8), simply because the definition provided by the Applicant relates also to the broader concept of charitable acts and not exclusively charitable entities, this does not preclude the string .Charity from having a strong association with the clearly delineated community of charities and charitable organisations.

5. The Interpretation of the Substantial Opposition Test

19. The factors to be considered under Article 3.5.4 of the Guidebook are only guidance and are not exhaustive or exclusive. Article 3.2.5 of the Guidebook gives the IO the right to object to an application if there is one comment in opposition to the application. The Applicant's criticisms of two of the public comments sharing the same language and three of them coming from the UK do not therefore detract from the IO's conclusion drawn in part from those comments or the Substantial opposition test (Response, p. 9).

20. The Applicant also mischaracterizes the concerns expressed in the comments (Response, p. 9). The comments relied upon in the Objection include the concern that the Application may potentially harm the system of trust on which charities and charitable giving are largely dependent (Objection, para. 29).

6. The Interpretation of the Detriment Test

21. The Applicant contends that the IO has not met his burden of proving the likelihood of material detriment or of the elements listed in Article 3.5.4 of the Guidebook (Response, pp. 11-13). Article 3.5.4 of the Guidebook lists "factors that could be used by a panel in making this determination [of the likelihood of material detriment]". However, this list is only guidance and is not limitative or exclusive.

22. What is striking is that, following the Applicant's reasoning, the IO should not prove a "likelihood of detriment", but bring "evidence of detriment" or "proof of harm" (Response, p. 12). This is to forget that during the *travaux* of ICANN concerning the new gTLD program and its guiding policy, it has been proposed that "evidence of detriment to the community or to users more widely must be provided".[9] This proposal has not been retained in the Final

[9] Proposed Implementation Guideline P (point h), reproduced in NCUC Minority Statement, Final Report of the Generic Names Supporting Organization (GNSO) on the Introduction of New Generic Top-Level Domains, 8 August 2007, Annex C, http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm#_Toc48210877.

Report of GNSO[10], not least in the Guidebook.. In this regard, one has to bear in mind that the dispute resolution procedure has been put into place in order to assess and to remedy in advance any potential negative effects of the operation of a new gTLD. By definition, detriment has not yet occurred as the gTLD has not yet been attributed and put into operation. The "likelihood of detriment" standard and the burden for the objector must be seen against this background. It is a risk assessment aimed at avoiding detriment for the community or parts of it.

23. Indeed, the Guidebook includes factors like the "[n]ature and extent of damage to the reputation of the community represented by the objector that *would* result from the applicant's operation of the applied-for gTLD string" (emphasis added). In particular, one of the factors confirms expressly that an objector has to demonstrate the "level of certainty that alleged detrimental outcomes would occur". If the Guidebook standards would require certainty as implied by the Applicant (Response, pp. 13-14), this last factor would remain without any concrete meaning and effect.

24. The IO has developed many elements establishing that there exists a likelihood of detriment, in particular because of the Applicant's unwillingness to propose preventive security measures assuring the charitable nature, the integrity and the trustworthiness of the entities represented and the information provided under the gTLD .Charity. Applicant continues to ignore the specificity of this string despite the fact that the GAC Beijing Communiqué of 11 April 2013 listed the .Charity gTLD within the "sensitive strings that merits particular safeguards" because this string is "likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm"[11]. The potential for harm if the .Charity gTLD were administered without mechanisms for protecting public trust in charities was likewise referred to by the IO (Objection, para. 39). Whatever the weight of its recommendations in the present proceedings, the GAC's Beijing communiqué is entirely consistent with the IO's concerns concerning the detriment the use of this application is likely to cause.

25. The Applicant states that the "Objector obtusely suggests a need for registration eligibility criteria, although without proposing what they might be" (Response, p. 13). However, Applicant should not benefit from the undefined nature of its own commitments in order to escape a Community objection under the likelihood of detriment test. It is not within the IO's remit to specify precisely what undertakings or commitments the Applicant should

[10] Implementation Guideline P Final Report of the Generic Names Supporting Organization (GNSO) on the Introduction of New Generic Top-Level Domains, 8 August 2007, http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm.

[11] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf, Annex I, Category 1, p. 8 (Annex 1).

make in order to avoid the likely detriment. Nevertheless, the IO provided a clear example of the type of measure that would reduce the likelihood of detriment, namely "stringent eligibility criteria established in advance in collaboration with the community and its stakeholders" (Objection, para. 48).

26. In this respect, the Applicant's enumerations of other safeguards are, although not unimportant, not directly relevant to the IO's recognition of a likelihood of material detriment. Further, the Applicant's reliance on existing standards is misplaced. The Guidebook standards are not aimed at reaching a mere "improvement" with regard to existing gTLDs and their rather weak protection mechanisms, but to avoid detriment to the community targeted.

27. Despite the detriment its position is likely to cause, the Applicant's ultimate parent continues to challenge the safeguard measures advised by the GAC[12], along the same lines as in this Application[13]. The Applicant, just like its ultimate parent[14], affirms its pro-open registry philosophy in its Response to IO's objection (Response, pp. 5, 9, 11 & 13).

Remedies Requested

The Independent Objector requests the Expert panel to hold that the present Objection is valid. Therefore, the Expert panel should uphold the present Objection against this .Charity Application.

In addition, the Independent Objector requests that its advance payments of costs shall be refunded in accordance with Article 14 (e) of the Procedure (Attachment to Module 3 - New gTLD Dispute Resolution Procedure).

Communication (Article 6(a) of the Procedure and Article 1 of the ICC Practice Note)

A copy of this Additional Written Statement is transmitted to the Applicant and its representatives on 22 August 2013 by e-mail to the following address: Contact Information Redacted

Contact Information Redacted

[12] http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf.

[13] Application, point 18 (a)

[14] See, e.g., Donuts' replies to the GAC Early Warnings of Australia (http://donuts.co/news/files/donuts_reply_to_australia_early_warning.pdf); France (http://donuts.co/news/files/donuts_reply_to_france_ARCHITECT_HEALTH_HOTEL_SARL_VIN.pdf); and Mali (http://donuts.co/news/files/donuts_reply_to_republic_of_mali.pdf). https://gtldcomment.icann.org/comments-feedback/applicationcomment/commentdetails/10236. https://gtldresult.icann.org/application-result/applicationstatus/applicationchangehistory:downloadtodocument/852?t:ac=656.

A copy of this Additional Written Statement is transmitted to ICANN on 22 August 2013 by e-mail to the following address: drfiling@icann.org

Description of the Annexes filed with the Objection (Article 8(b) of the Procedure)

List and Provide description of any annex filed.

Annex 1: GAC Advice, Beijing Communiqué, 11 April 2013, http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf

Date: 22 August 2013

Signature: ______________________

Attachment 4

[Corn Lake Sur-Reply]

International Chamber of Commerce
The world business organization

International Centre for Expertise   Centre international d'expertise

NEW GENERIC TOP-LEVEL DOMAIN NAMES ("gTLD") DISPUTE RESOLUTION PROCEDURE

ADDITIONAL WRITTEN STATEMENT OF APPLICANT CORN LAKE, LLC

Disputed gTLD

gTLD Applicant has applied for and Objector objects to:

Name	<.CHARITY> – Application ID 1- 1-1384-49318
ICC Case No.	ICC Case No. EXP/395/ICANN/12

INTRODUCTION

Objector's August 22, 2013 additional submission ("Reply") suffers from the same infirmity as the original Objection: it offers no evidence to meet Objector's significant burden to prove all four elements required by the Guidebook for a valid community objection. The Reply remains as speculative and lacking in evidence as the original Objection.

Instead of taking the Reply opportunity to provide meaningful *facts* and *evidence* to support his claims, the IO argues little more than that Applicant has misinterpreted the applicable Guidebook provisions. It is Objector, however, who misconstrues the four tests that must all be met to prevail on a community objection.

Objector even goes so far as to state that he need not even *present* the proof that Applicant (and the Guidebook) says he must. Reply ¶ 22 n.10. The Guidebook, however, could not state more clearly that "[t]he objector bears the burden of *proof* in each case." AGB § 3.5 (emphasis added). This requires *evidence*: "Evidence is appropriately required in all types of objection proceedings. Absent evidence, no objection should stand." http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf.

The only "evidence" the IO offers concerns an April 2013 "communiqué" from ICANN's Government Advisory Committee ("GAC"). The GAC's statements, however, have no relevance to and do nothing to bolster the Objection. Rather, the ICANN Board must

© International Chamber of Commerce (ICC) D 2012. All rights reserved. No part of this document may be reproduced or copied in any form or by any means, or translated, without the prior permission in writing of ICC.

determine what GAC recommendations to accept and additional “protections” to implement, and Applicant will have to abide by any such decision. That *policy* determination properly rests with the ICANN Board, not the Objector or this Panel.

Regardless of the GAC Beijing communiqué, neither the Objection nor the Reply offers sufficient evidence to discharge Objector’s burden to prove *all four* community objection elements – *i.e.*, to demonstrate that *each* is more likely than not true. As such, the Objection – based on unsubstantiated fear, speculation, and conjecture – must be denied. AGB at 3-25.

ARGUMENT

Applicant’s parent, Donuts, has passed ICANN’s Initial Evaluation (IE) on this and every other one of its more than 300 applications. Supp. Nevett Dec. ¶ 4 (**Annex 1** hereto). Moreover, ICANN already has entered into thirteen new registry agreements with Donuts to operate 13 of the first 18 new gTLDs awarded to date. Having so demonstrated its qualifications to operate a registry, Applicant has the presumptive right to compete with the other applicants for the <.CHARITY> gTLD, and Objector bears the “corresponding burden … to show why that gTLD should not be granted to the [A]pplicant." http://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf.

Specifically for purposes of this community Objection, the IO must prove: (i) a clearly delineated community; (ii) substantial opposition from that community; (iii) a strong association between the community and the applied-for string; and (iv) material detriment to the community caused by Applicant’s operation of the string. AGB § 3.5.4. He must satisfy *all four* criteria to prevail. *Id.* at 3-25.

The IO remains deficient on each of these standards. He improperly conflates the “clearly delineated” and “strong association” (“targeting”) tests, and presents no evidence to demonstrate either. He claims to have met the “substantial opposition” test simply by having chosen to object, and presents no evidence to augment the inadequate showing made in his original Objection.

Finally, the IO presents no evidence to satisfy his burden to *prove* a “likelihood” of “material detriment” to the “rights or legitimate interests” of a “significant portion” of any “community” denoted by the word “charity.” Instead of taking the opportunity to provide *facts* and *evidence* to support his claims of potential "detriment," Objector again relies solely on speculation as to what hypothetical third parties *may* do with the domain at some later time. He argues for registration restrictions, including “stringent eligibility criteria,” without identifying any specific measures or how a <.CHARITY> registry operator should implement them. Instead, the IO dismisses the need to present evidence on such issues as “not within his remit," Reply ¶ 25, notwithstanding that he bears the burden of proof. AGB at 3-18.

Nor do the IO’s (unsubstantiated) calls for registration barriers justify why ordinary people who participate or have an interest in charitable activities, as well as journalists, database aggregators, religious groups, foundations, charitable arms of for-profit entities, and others that may use the gTLD in a lawful manner, should not have the ability to register a <.CHARITY> domain. Would http://www.charity.com, which appears to serve as a directory for charities in numerous areas such as addiction, disaster relief and homelessness, be restricted in the IO’s policy preference? ICANN did not appoint the IO to make new policy that he prefers to replace the policies agreed upon by ICANN’s multi-stakeholder process. The IO, at times, appears to have lost his mission.

Indeed, the registry limitations the IO advocates would *cause* material harm to the public by restraining the fundamental rights of free and lawful expression. Such a scheme has no place on the Internet, especially with regard to a dictionary word like “charity.” The IO conveniently ignores all of the protective mechanisms that ICANN requires, those that

Donuts has added voluntarily, and all new safeguards that ICANN recently implemented based on the GAC's Beijing comments (and which Donuts supported publicly).

Such overreaching, coupled with the fact that the IO has devoted the bulk of his efforts toward gTLDs applied for by Donuts in particular, has caused Applicant to question the Objector's true independence. Applicant has nothing further to add on that subject, and leaves it to the Panel to deny the Objection for its lack of merit, regardless of the IO's motives in bringing it.

Objector Again Fails to Demonstrate Any "Clearly Delineated" Charity "Community" That the String "Targets."

Rather than proffer evidence that some "clearly delineated" charity "community" actually exists, and that a <.CHARITY> string "targets" it, the IO demurs that Applicant misconstrues the Guidebook's "clearly delineated" standard and muddles it with the "targeting" test. Reply ¶¶ 11-18. However, Applicant has done nothing of the sort.

The word "charity" does not "clearly delineate" any "community."

Applicant has applied a universally accepted principle of construction to show that the Guidebook includes a different, and logically more stringent, test for "clearly delineated" under the substantive merits of the objection than that used for determining standing. Resp. at 7. ICANN would have had no need to include a separate "clearly delineated" test on the merits if it meant nothing more than the showing an objector already would have had to make on standing. *Id.* It therefore must have meant that the two tests have different metes and bounds. Objector argues that such widely-recognized analytical techniques would render the "targeting" test meaningless. Reply at 12.

This overly simplistic argument fails. ICANN's multiple stakeholders expressed the intent when formulating the Guidebook that the challenged string itself indeed must describe or "clearly delineate" a "community." They designed the community objection as a vehicle "to prevent the *misappropriation* of a string that *uniquely or nearly uniquely* identifies a well-established and *closely connected group* of people or organizations." *See* http://archive.icann.org/en/topics/newgtlds/agve-analysis-public-comments-04oct09-en.pdf at 19 (emphases added).

Under this standard, Objector's purported "community" of "all charitable institutions," Obj'n ¶ 11, simply cannot pass muster. The term charity is broader than just charitable institutions. Individuals may want to blog about their charitable endeavors or simply donate space on their website to worthy charities;[1] for-profit businesses may want to establish a website to discuss their giving;[2] suppliers and advisors to charitable institutions may want to advertise their services;[3] or even individuals with the name "Charity" might want to use the TLD.[4] Whether or not a <.CHARITABLEINSTITUTION> gTLD might describe Objector's purported community, the broader string <.CHARITY> makes no such delineation.

The Guidebook invites a Panel to consider the level of "formal boundaries around the community." Not only does Objector fail to articulate exactly how to define a "charitable institution" or how to deal with the malleability of such a generic and widely-applicable term,

[1] *See, e.g.,* UK-based "Atomic Shrimp," a blogger who donates ad space on his website simply "because he can." http://www.atomicshrimp.com/st/content/advertise/.

[2] *See, e.g.,* "Charity begins at work: Taking Corporate Responsibility Seriously" available at: http://www.theguardian.com/voluntary-sector-network-zurich-partner-zone/charity-begins-at-work (last accessed Sept. 5, 2013).

[3] *See, e.g.,* www.likecharity.com, a technology company that provides I.T. solutions for charities/non-profits that seek donations via mobile phones and social media websites.

[4] *See* http://charitysplace.wordpress.com (a blog maintained by author Charity Bishop).

he even specifically dismisses the task as totally unnecessary, notwithstanding that he alone bears the burden of proof. The IO thus appears to articulate a “loosely delineated” standard at best, such that one cannot determine what “institutions” would make up the “community.” For example, would Toronto's "Charity Village," an HR placement provider that matches qualified candidates with positions at Canadian non-profit organizations[5] qualify as a "charitable institution” under the IO's standard?

Indeed, Objector does not even limit the Objection to "licensed" or "regulated" organizations as one might gather from the Reply, but instead more broadly references "*all* charitable institutions, *including* those that are specifically registered or regulated in some form in the states where they operate." Obj’n ¶ 11 (emphasis added). So, on the one hand, Objector urges the Panel to cordon off access to a domain making use of a dictionary word, while at the same time dismissing the need to specify exactly who makes up the "community" that should have such access. Objector cannot have it both ways and satisfy his burden.[6]

Objector’s reference to GAC comments does not overcome his absence of proof. While we discuss the GAC’s lack of impact on these proceedings in greater detail *infra*, nothing suggests that the GAC specifically views a <.CHARITY> TLD as denoting a “community,” as opposed to simply one of many “sensitive strings.” The GAC mentioned *hundreds of* strings in its Beijing advice, for the purpose of suggesting possible additional "safeguards" for those gTLDs – not to advise ICANN to create a community resulting in rejection of all non-community applicants. Just like the GAC did not intend to create a community by mentioning <.DIET> or <.CARE>, the GAC does not and cannot create a community for <.CHARITY>.

Objector has not satisfied the separate “targeting” test.

Objector contends in the Reply that Applicant’s interpretation of the “clearly delineated” test would make it indistinguishable from the “strong association” or “targeting” standard. This ignores that the “strong association” or “targeting” test does not look solely at the generic association between the string and the “community” in the eyes of the public. It also expressly considers what the *Applicant* “targets,” as the Guidebook factors under this element include “[s]tatements contained in the application” and “[o]ther public statements by the applicant.” AGB at 3-24. Thus, the Guidebook by its terms distinguishes the “strong association” and “clearly delineated” standards.

Regarding the third targeting factor of “public association” of <.CHARITY> with a “community,” Objector continues to discount the generic nature of the string. Users can employ a <.CHARITY> domain in a variety of perfectly legitimate ways, as they do today at the second level of existing gTLDs. As examined above, boundless examples could include: (i) www.charity.com (which provides "information about charities and nonprofit organizations, services, donations, resources, volunteer opportunities"); (ii) www.taxfreecharity.com (a provider of incorporation and tax services specifically designed for charitable and non-profit organizations); (iii) www.ticketsforcharity.com (a ticket broker that obtains premium tickets and preferred access passes from musicians, professional sports teams, theaters and other entities, and donates proceeds to various charities); (iv) www.gocharity.com (a marketing and public relations company that assists charities and non-profits with hosting auctions for donated items to raise funds); (v) www.100chicksforcharity.com (a women's social club in Des Moines, Iowa that organizes meetings to raise awareness about ways people can donate and help charities in their city); (vi) www.scaryforcharity.com (an annual Halloween

[5] *See* http://charityvillage.com.

[6] One of the factors for determining a “clearly delineated community” is its level of "public recognition." AGB at 3-22. Can the public readily distinguish what is and what is not a "charitable institution" in the same way that it might identify someone of African descent, a Sunni Muslim, or a commercial airline pilot? Even if it could, the Objection challenges the gTLD <.CHARITY> and not <.CHARITABLEINSTITUTION>.

party and costume contest that donates money obtained from ticket sales and sponsorships to local children's charities); (vii) www.hellohumankindness.org (a website offering tips on how, quite simply, to be nice to one another); (vii) www.voolla.org (a database of people offering their skills for free to charitable causes); or perhaps (viii) the "CHARITY" computer programming language (http://en.wikipedia.org/wiki/Charity_programming_language).

The public might well not “strongly associate” such diverse constituencies with the generic term “charity.” Yet, Applicant’s approach to a <.CHARITY> registry would include all of them. Applicant would “target” such widely varied interests that one simply cannot define as a “clearly delineated community.”

Like the Objection, the Reply Demonstrates No “Substantial Opposition.”

The Reply attempts to circumvent the IO’s failure to prove “substantial opposition” by a “significant portion” of an alleged “charity” community. The IO contends that Guidebook factors “are only guidance and are not exhaustive or exclusive,” and that his “right to object to an application if there is one comment in opposition to the application” means that he satisfies this element with even a single opposition. Reply ¶ 19, citing AGB §§ 3.2.5, 3.5.4. However, that a purportedly adverse comment may give the IO *standing* to object does not obviate his burden to prove the “substantial opposition” prong of the Objection substantively. Whether or not “exhaustive or exclusive,” the Guidebook factors are not met by little or no showing at all.

Objector has cited a handful of negative comments about a prospective <.CHARITY> domain, almost all – *i.e.*, three or four – from the UK, Scotland and Wales. This does not amount to “substantial” opposition from a “significant portion” of any charity “community.”

Objector Mischaracterizes the "Material Detriment" Standard in a Misplaced Effort to Justify Having Failed to Satisfy It.

Objector still provides no *proof* that the Application *itself* “creates a *likelihood* of *material* detriment to the *rights* or *legitimate interests* of a significant portion of” the alleged “charity” community. AGB at 3-24 (emphases added). Rather, he continues to cite Applicant's purported unwillingness to propose preventative measures as his primary reason for objecting. Reply ¶ 25, completely ignoring the eight protective mechanisms that the Application undertakes *in addition to* the fourteen steps that ICANN *already* requires for *new* gTLDs *over and above* what it demands of *existing* gTLDs, the *four further* measures Applicant will implement due to the sensitivity it acknowledges as to this particular string, and its support of even more safeguards coming out of the GAC Beijing communiqué. *See* Response **Annex B**: Nevett Dec. ¶¶ 11-12 and *Ex. 1* at 8-9 [Application § 18(a)]. *See also* Applicant’s support at http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf.

Objector’s unsubstantiated accusation of Applicant’s unwillingness to adopt certain “additional conditions” to safeguard a <.CHARITY> domain, run headlong into evidence proving directly the opposite:

> By applying our array of protection mechanisms, Donuts will make this TLD a place for Internet users that is far safer than existing TLDs.
>
> [Listing of 26 safeguards follows – 14 required by ICANN beyond those imposed on existing gTLDs, 8 more voluntarily adopted by Donuts to add additional protections to all of its applied-for gTLDs, and 4 additional protections directed specifically to <.CHARITY> as a “sensitive” domain.]

Resp. **Annex B**: Nevett Dec. ¶¶ 8-12, Ex. 1 ¶ 18(a) at 7-9 (emphases added). Objector at no time rebuts these or the many other statements throughout the Application that flatly negate the concerns raised in the Objection.

Objector skirts dealing with these adverse facts directly, Instead, he suggests that the Guidebook does not actually require objectors to provide evidentiary support for their arguments, as a "proposal" requiring "[e]vidence of detriment to the community" supposedly did not make it into the Implementation Guidelines of ICANN's Generic Names Supporting Organization ("GNSO") that initiated the new gTLD program back in 2007. Reply ¶ 22 n.10.

This argument is verifiably inaccurate. Indeed, the IO himself links to the final guidelines, http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-para-08aug07.htm, which clearly state that "the objector *must* provide sufficient *evidence* to allow the panel to determine that there would be a likelihood of detriment to the rights or legitimate interests of the community or to users more widely." (Emphases added.) Subsequently, the multiple stakeholders who developed the Guidebook required "[e]vidence … in all types of objection proceedings," stating that, "[a]bsent evidence, no objection should stand." http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf.

Also, the GNSO just makes policy *recommendations* to the ICANN Board. The ICANN Board and stakeholders then take those aspects into account in establishing the Guidebook, and the Guidebook ultimately controls – not five year old recommendations. In fact, the Guidebook itself as ultimately issued in 2012 could not state more clearly: "The objector bears the burden of *proof* in each case." AGB § 3.5 (emphasis added). The IO cannot evade this obligation.

Ultimately, Objector's "detriment" claim boils down to his disagreement with Applicant's "open registry" approach. However, the choice to run an "open" (or even closed) gTLD does not form part of the *community objection standard.* Objector cites no Guidebook provision that stands for such a proposition, because none exists. Nothing in the Guidebook requires an applicant to run a registry to benefit any particular "community," or to restrict its registrations to "approved" registrants only. Yet, even the IO concedes that no applicant must operate a <.CHARITY> gTLD only as a community: "The Guidebook does not require that any and every gTLD string . . . must necessarily be applied for by a representative of the community." Reply ¶ 7.

Further, Objector's quarrel with Applicant's open registry policy ignores the material harm inflicted upon the public from *restricting* access to a generic TLD such as this. Barring all but verifiable "charitable institutions" (whatever that expression is deemed to mean) not only quashes free speech rights, but also cuts off benefits to charitable interests by artificially excluding, among many others, those who provide services to, gather and disseminate information about, or donate to and comment on charities. Objector's position restrains speech and stunts the growth of the domain name system, thus thwarting two of the primary, stated goals of ICANN's new gTLD program.

Such real, immediate and readily identifiable harms resulting from the entry barriers that the IO seeks contrast sharply with the remote possibility of future harm about which he conjectures. Such vague and speculative notions do not meet the IO's burden to prove a "likelihood" of "material detriment" to a "community" that even he cannot define. This utter lack of proof defeats the Objection. AGB at 3-24, 3-25.

The GAC Beijing Communiqué Adds Nothing to the Objection.

Objector places great weight on the GAC's Beijing communiqué, when in fact it has no relevance to the Objection. If it did, it would compel the Objection's denial.

Objector incorrectly asserts that the "concerns" he has expressed about a <.CHARITY> string have been "confirmed" by the GAC's Beijing communiqué, most notably with respect to registration restrictions. Reply ¶ 17. However, the GAC's comments from Beijing identified *hundreds of* strings, without reference to any particular applicant or application, which it believed generally should have "additional safeguards." Indeed, the GAC stated that it recommends registration restrictions for only "some" of the listed strings, without identifying <.CHARITY> or any other as among them. Also, the GAC merely expressed "concerns" about such undifferentiated strings. It *did not* say they should not go forward. Objector cannot attribute any specific GAC suggestion to <.CHARITY>, and cannot use the GAC statements to deny Applicant the opportunity to compete for the string.

The Panel can confirm the foregoing from the document itself, Reply Annex 1, as opposed to Objector's characterization of it, Reply ¶ 17. The Panel also can confirm that Applicant *supports* much of the GAC's general advice on so-called "sensitive strings." *See* http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf ("The Board should accept most of the GAC advice and work toward implementation"). Objector simply ignores this to the extent it contends otherwise. In fact, as detailed below, Applicant ultimately will contractually bind itself to whatever GAC recommendations ICANN adopts.

The Beijing advice does not extend nearly to the lengths that Objector would have this Panel go, most notably with respect to "safeguards" versus "registration restrictions." Current policy, as expressed in the Guidebook, does not require the onerous registration constraints for which Objector advocates. Applicant has stated its respectful disagreement with the GAC's suggestion that certain strings "may require . . . clear and/or regulated entry requirements." Applicant has long held and stated the position that artificial restrictions placed on otherwise legitimate registrants seeking domains such as <.CHARITY>, which deal with generic forms of activity and expression, unnecessarily curtail free speech and run contrary to ICANN's stated goals of maximizing Internet participation. AGB Preamble and § 1.1.2.3; Resp. **Annex B**, Exh. 1 at ¶ 18. However, if the GAC ultimately does urge such measures for the string at issue, and the Board accepts the GAC's policy advice, Applicant of course would, as it must, abide by that decision. It is a *policy* decision, however, to be made by the *ICANN Board* and not by Objector or even this Panel.

The Reply misapprehends the GAC's role and advice, the Applicant's policy position, and the effect of GAC recommendations on the instant Objection. The Guidebook provides that the GAC may provide "advice" to the ICANN board to "address applications that are identified by governments to be problematic, *e.g.,* that potentially violate national law or raise sensitivities." AGB § 3.1. "GAC Advice" may take one of three forms:

(i) "that a particular application *should not proceed*," which "will create a *strong presumption* for the ICANN Board that the application should not be approved;"

(ii) that the GAC has "*concerns*" about a particular string, as to which t ICANN board may "*enter into dialogue* with the GAC to understand the scope of" said "concerns," then decide what to do about them and "provide a rationale for its decision;" or

(iii) "that an application *should not proceed* unless remediated," which "will raise a *strong presumption* for the Board that the application should not proceed" absent such remediation.

Id. (emphases added). The Beijing communiqué merely expressed "concerns" regarding potentially “sensitive strings” (such as <.CHARITY>) corresponding to the *second* form of GAC advice, which does not call for rejection of the string or even “create a strong presumption” that such as a result should occur, whether outright or absent remediation. *Id.*

As such, ICANN does not have any specific obligation to accept all or any of the Beijing recommendations regarding the subject string. It already has accepted much of the GAC advice, changed Registry Agreements, and also must "enter into dialogue with the GAC to understand the scope of concerns" — which is has now done — and "provide a rationale for” whatever it ultimately decides. *Id.* If the Board rejects the GAC's concerns about registration restrictions, then Applicant would have no obligation to address them. If instead ICANN incorporates such concerns into resolutions, Applicant would have the obligation to implement them.

In any event, Applicant has explicitly recognized <.CHARITY> as a "sensitive" string, and as a result voluntarily taken on additional protective measures over and above the *fourteen* required by ICANN for other New gTLDs, and the *eight more* that Donuts will adopt for all its "non-sensitive" applications. A <.CHARITY> gTLD run by Applicant will be safer than most any gTLD the Internet has ever known, and a leader among *all* new gTLDs in that respect.

While Applicant supports the vast majority of the GAC's *safeguards,* it disagrees with the policy position taken by the IO on registration *restrictions,*[7] and would generally permit the public to engage in free expression if and to the extent that it does not violate the law, at which time the Applicant would take swift action. Objector tries to use Donuts’ policy of not restricting speech *ex ante*, and taking action against any unlawful speech *ex post*, as itself grounds for a valid objection. This ignores what the subject Application specifically provides:

> This TLD is attractive and useful to end-users as it better facilitates search, self-expression, information sharing and the provision of *legitimate* goods and services.
>
> * * * * *
>
> In order to avoid harm to *legitimate* registrants, Donuts will not artificially deny access (*without legal cause*), to a TLD that represents a generic form of activity and expression.
>
> * * * * *
>
> Restrictions on second level domain eligibility would prevent *lawabiding individuals and organizations* from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD.

See Resp. **<u>Annex B</u>**, Exh. 1 ¶ 18(a). While the IO disagrees with this different means to the same end of protecting lawful activity, such a policy position lies beyond his mandate and simply does not discharge his burden or comport with the express standards of the Guidebook.

The GAC “advice,” therefore, has little (if any) bearing on the material detriment analysis. ICANN in fact *has* accepted much of the protections suggested by the GAC at

[7] It is also worth noting that the IO often employs the term "safeguards" liberally as also encompassing his favored registration restrictions, *see* Reply ¶ 27, despite the fact that the GAC treated the latter quite differently. *See* http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf (Annex 1) at pages 8-9 ("safeguards" generally) and at page 10 (registration restrictions).

Beijing, and remains in “dialogue” with GAC on the specific means of doing so with respect to potentially sensitive “Category 1” strings. Nevett Supp. Dec. ¶ 2 and Ex. A (**Annex 1** hereto). Whatever specific measures ICANN enacts will require implementation by Applicant in the form of a PIC, then embodied in a formal registry agreement by which Applicant must bind itself to undertake those measures under penalty of losing the registry. Donuts speaks from factual experience, as it already has entered into such agreements for thirteen strings that ICANN has thus far awarded it. *Id.* ¶ 3 and Ex. B.

The IO exceeds his authority when referencing GAC advice. The ICANN Board will decide what it will and will not accept as a matter of policy. This will moot the IO’s reliance on the advice to “prove” detriment. The Board will have determined the protections it will require and the risks it will allow. Neither the Objector nor the Panel can properly don such a policy mantle. ICANN has defined the tasks of both by the standards specified in the Guidebook. They dictate the showing that the IO must but has failed to make. Because the IO has presented mere speculation and conjecture simply by negative inference from inapposite GAC advice, rather than actual *evidence* sufficient to carry its burden to *prove* a “likelihood” of “material detriment,” the Panel must reject the Objection.

CONCLUSION

Objector not only exceeds the bounds of the Guidebook; he infringes upon the free speech rights of Applicant and the general public. An average consumer may want to discuss and critique various “charities," or conduct humanitarian activities to benefit society. Should these persons have to obtain prior permission or "show their papers" in order to do so? This notion seems completely lost on the Objector. To argue that sustaining the Objection would not amount to an impingement of such rights (Reply ¶ 9) amounts to a *prior restraint* — often considered to be one of the most severe and unjustifiable means of curtailing expression.[8]

The Panel must decide within Guidebook constraints, based on the evidence before it and the burden of proof placed on the Objector. The Objection fails to satisfy the substantive objection standards or his burden of proof. For these reasons, all as demonstrated more fully above and in its original Response, Applicant again respectfully urges the Panel to reject the ill-advised Objection.

DATED: September 6, 2013

Respectfully submitted,

THE IP & TECHNOLOGY LEGAL GROUP, P.C.
dba New gTLD Disputes

By: _____/jmg/____________
John M. Genga
Contact Information Redacted

By: _____/dcm/____________
Don C. Moody
Contact Information Redacted

Attorneys for Applicant/Respondent
CORN LAKE, LLC

[8] *See, e.g.,* the U.S. Supreme Court Decision in the "Pentagon Papers" case: *New York Times Co. v. United States*, 403 U.S. 713 (1971) *copy available at:* http://bit.ly/1cDsvJk; *see also* decision by the European Court of Human Rights in *Ahmet Yildirim v. Turkey* (no.3111/10), *available at:* http://bit.ly/11zBeZS (French) and http://bit.ly/YgCQXh (English).

Communication (Article 6(a) of the Procedure and Article 1 of the ICC Practice Note)

A copy of this Response is/was transmitted to the Objector on: September 6, 2013

Contact Information Redacted

Contact Information Redacted

and

A copy of this Response is/was transmitted to ICANN on September 6, 2013 by e-mail to the following address: DRfiling@icann.org.

Description of the Annexes filed with the Response (Article 11(e) of the Procedure)
List and Provide description of any annex filed.

Annex 1 – Supplemental Declaration of Jonathon Nevett

Exhibit A – http://www.icann.org/en/news/announcements/announcement-2-03jul13-en.htm, 3 July 2013 New gTLD Program Committee Progress on Addressing GAC Beijing Advice on New gTLDs

Exhibit B – Donuts Registry Agreement for .CAMERA

Annex 1

[Supplemental Declaration of Jonathon Nevett]

DECLARATION OF JONATHON NEVETT

I, Jonathon Nevett, declare as follows:

1. This declaration supplements my June 22, 2013 declaration in this matter, and supports applicant Corn Lake, LLC's Response to Objector's Additional Written Statement herein. I make the statements herein from my own personal knowledge.

2. I personally participated in responding to the communiqué issued by ICANN's Government Advisory Committee (GAC) at Beijing on April 11, 2013. As such, I also personally have followed ICANN's decisions concerning the recommendations in the GAC communiqué. Included herewith as Exhibit A is a true and correct copy of a publicly available July 3, 2013 report by the ICANN Board New gTLD Program Committee ("NGPC") regarding its "Progress on Addressing GAC Beijing Advice on New gTLDs." Starting at Item number 13 of the chart contained therein, the report reflects that the NGPC has accepted the GAC's six recommendations regarding safeguards for all gTLDs (Items 13-18), and remains in "dialogue" with the GAC regarding the eight measures proposed by the GAC with respect to the "Category 1" strings referenced in the communiqué, including <. CHARITY > (Items 19-26).

3. Donuts supports much of the GAC Advice from Beijing. I am very familiar with what Donuts must do to implement any items of GAC Advice accepted by the ICANN Board. Donuts must make a "Public Interest Commitment" or "PIC" to adhere to each such recommendation, which then get embodied in a Registry Agreement with ICANN for the subject string. Donuts, in fact, already has done this for its first string. Included herewith as Exhibit B is a true and correct copy of its publicly available Registry Agreement for the gTLD for "CAMERA." Specification 11 starting at page 87 of that Registry Agreement sets forth Donuts' PICs for that string. Section 4.3(e) at page 11 of the Registry Agreement allows ICANN to terminate the

agreement should Donuts breach the PICs set forth in Specification 11. On August 30, 2013, Donuts signed similar registry agreements with ICANN for an additional twelve (12) strings.

4. Donuts has passed all of the Initial Evaluations conducted by ICANN on its applications to date, with zero failures.

I declare under penalty of perjury under the laws of the United States that based on my personal knowledge and belief the foregoing is true and correct and that this declaration was executed by me on September 6, 2013, in Rockville, Maryland, USA.

__________/jn/______________________
Jonathon Nevett

Exhibit A

[3 July 2013 New gTLD Program Committee Progress on Addressing GAC Beijing Advice on New gTLDs]

ICANN

Internet Corporation for Assigned Names and Numbers

Menu Help

NEWS & PRESS › ANNOUNCEMENTS

NGPC Progress on Addressing GAC Beijing Advice on New gTLDs

3 July 2013

On 2 July 2013, the the ICANN Board New gTLD Program Committee (NGPC) had its seventh meeting to discuss the GAC Beijing advice on New gTLDs. The Committee took the following actions:

1. Initial Protections for IGO Protections

   In the Beijing Communiqué, the GAC reiterated previous advice that "appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch." In response to a number of issues raised by the Board, the GAC noted in the Beijing Communiqué that it is "mindful of outstanding implementation issues" and that it is committed to "actively working with IGOs, the Board, and ICANN Staff to find a workable and timely way forward. In a 6 June 2013 response letter to the GAC on the IGO GAC Advice, the ICANN Board Chairman proposed that a small number of NGPC members and ICANN staff begin a dialogue with the GAC on these issues

   At its 2 July 2013 meeting, the NGPC passed a resolution confirming that the New gTLD Registry Agreement will require operators to provide appropriate preventative initial protection for the IGO identifiers. These protections will remain in place while the GAC, NGPC, ICANN Staff and community continue to actively work through outstanding implementation issues. More specifically, registry operators will implement temporary protections for the IGO names and acronyms on the "IGO List dated 22/03/2013" until the first meeting of the NGPC following the ICANN 47 Meeting in Durban. The Resolution provides temporary protections for IGOs while respecting the ongoing work on implementation issues. The IGO List is attached to the Resolution as Annex 1.

   ICANN Network Acronym Helper Help

   If the NGPC and GAC do not reach an agreement on outstanding implementation issues for protecting IGO names and acronyms by the first meeting of the NGPC following the ICANN 47 meeting in Durban, and subject to any matters that arise during the discussions, registry operators will be required to protect only the IGO names (and not the acronyms) identified on the GAC's IGO List.

2. Category 1 Advice

   In the Beijing Communiqué, the GAC proposed Category 1 safeguard advice, which includes recommended restrictions and consumer protections for sensitive strings and regulated markets. The Category 1 Safeguard Advice is divided into three main sections. The first section provides five (5) items of advice that apply to "strings that are linked to regulated or professional sectors." The Beijing Communiqué identified a list of strings to which this advice applies. The second section provides three (3) additional pieces of advice that should apply to a limited subset of the strings noted in the GAC's list that are "associated with market sectors which have clear and/or or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions…." The third section includes an additional requirement for applicants for the following strings: .fail, .gripe, .sucks and .wtf.

On 23 April 2013, ICANN initiated a public comment forum to solicit input on how the NGPC should address GAC advice regarding safeguards applicable to broad categories of new gTLD strings http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm. The public comment forum closed on 4 June 2013. While many commenters voiced support for the Category 1 safeguard advice, many others submitting opposing comments. One overarching theme from the public comments was the need for additional clarity on the scope and intent of the Category 1 Safeguard Advice.

After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice.

3. New gTLD Registry Agreement

Finally, the NGPC considered the revised New gTLD Registry Agreement that will be entered into between ICANN and successful new gTLD applicants. The revised agreement is the result of several months of negotiations, formal community feedback (most recently during public comment forums initiated on 5 February 2013 on 29 April 2013), and meetings with various stakeholders and communities. The revisions include feedback from the ICANN community at the ICANN 46 Meeting on 7-11 April 2013 in Beijing as well as GAC advice issued in its Beijing Communiqué.

After considering the comments received from the community, the NGPC determined that the revised New gTLD Registry Agreement included significant improvements in response to the concerns raised by the community. The Committee also noted that in response to the GAC's Beijing Communiqué, revisions were made to Specification 11 to implement the non-Category 1 safeguard advice (i.e., safeguards applicable to all strings and Category 2 safeguards). The revisions to Specification 11 incorporate standardized language to address the safeguard advice. Applicant-specific PICs will be included on a case-by-case basis to the extent not superseded by or inconsistent with the standard PICs included to address the GAC's Beijing Communiqué.

The NGPC approved the form of the New gTLD Registry Agreement and authorized ICANN staff to take all necessary steps to implement it and to move forward with implementation of the New gTLD Program. The Agreement is attached to the Resolution as Annex 1; the complete Summary of Changes to the New gTLD Registry Agreement is attached to the Resolution as Annex 2; a redline of the current agreement as compared to the previous version dated 29 April 2013 is attached to the Resolution as Annex 3; and the Summary and Analysis of Public Comments is available at http://www.icann.org/en/news/public-comment/report-comments-base-agreement-01jul13-en.pdf [PDF, 338 KB].

All of the resolutions adopted at the 2 July 2013 NGPC meeting are posted at http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm. A table summarizing NGPC Consideration of the GAC's Beijing Advice appears below.

GAC Register #	Summary of GAC Advice	NGPC Position	NGPC Response
1. 2013-04-11-Obj-Africa (Communiqué §1.a.i.1)	The GAC Advises the ICANN Board that the GAC has reached consensus on GAC Objection Advice according to Module 3.1 part I of the Applicant Guidebook on the following application: .africa (Application number 1-1165-42560)	Accept	• Applicant was permitted to withdraw or seek relief according to ICANN's accountability mechanisms subject to the appropriate standing and procedural requirements. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
2. 2013-04-11-Obj-GCC (Communiqué §1.a.i.2)	The GAC Advises the ICANN Board that the GAC has reached consensus on GAC Objection Advice according to Module 3.1 part	Accept	• Applicant was permitted to withdraw or seek relief according to ICANN's accountability mechanisms subject to the appropriate standing and procedural requirements. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-

	I of the Applicant Guidebook on the following application: .gcc (application number: 1-1936-2101)		en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
3. 2103-04-11-Religious Terms (Communiqué §1.a.ii)	The GAC Advises the Board that with regard to Module 3.1 part II of the Applicant Guidebook, the GAC recognizes that Religious terms are sensitive issues. Some GAC members have raised sensitivities on the applications that relate to Islamic terms, specifically .islam and .halal. The GAC members concerned have noted that the applications for .islam and .halal lack community involvement and support. It is the view of these GAC members that these applications should not proceed.	Accept	- Pursuant to the requirements of Section 3.1.ii of the AGB, NGPC and GAC members will enter into a dialogue on this matter in Durban. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
4. 2013-04-11-gTLDStrings (Communiqué §1.c)	In addition to this safeguard advice, the GAC has identified certain gTLD strings where further GAC consideration may be warranted, including at the GAC meetings to be held in Durban. Consequently, the GAC advises the ICANN Board to not proceed beyond Initial Evaluation with the following strings : .shenzhen (IDN in Chinese), .persiangulf, .guangzhou (IDN in Chinese), .amazon (and IDNs in Japanese and Chinese), .patagonia, .date, .spa, . yun, .thai, .zulu, .wine, .vin	Accept	- ICANN has allowed evaluation and dispute resolution processes to go forward, but will not enter into registry agreements with applicants for the identified strings for now. - NGPC expects GAC to consider these applications further in Durban. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
5. Request for Written Briefing (Communiqué §1.d)	The GAC requests a written briefing about the ability of an applicant to change the string applied for in order to address concerns raised by a GAC Member and to identify a mutually acceptable solution.	Provided	Written briefing provided at https://gacweb.icann.org/download/attachments/28278832/NGPC%20Scorecard%20of%201As%20Regarding%20Non-%C2%ADSafeguard%20Advice%20in%20the%20GAC%20Beijing%20Communique%CC%81.pdf?version=1&modificationDate=1372384291000&api=v2 [PDF, 2.68 MB]
6. 2013-04-11-CommunitySupport (Communiqué §1.e)	The GAC advises the Board that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such	Accept	- Criterion 4 for the Community Priority Evaluation process takes into account "community support and/or opposition to the application" in determining whether to award priority to a community application in a contention set. - If a contention set is not resolved by the applicants or through a community priority evaluation then ICANN will utilize an auction as the objective method for resolving the contention.

	opinion should be duly taken into account, together with all other relevant information.		See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
7. 2013-04-11-PluralStrings (Communiqué §1.f)	The GAC believes that singular and plural versions of the string as a TLD could lead to potential consumer confusion. Therefore the GAC advises the Board to reconsider its decision to allow singular and plural versions of the same strings.	Accept	• After careful consideration of the issues, review of the comments raised by the community, the process documents of the expert review panels, and deliberations by the NGPC, the NGPC determined that no changes to the ABG are needed to address potential consumer confusion specifically resulting from allowing singular and plural versions of the same strings. • The NGPC considered several significant factors during its deliberations about whether to allow singular and plural version of the same strings. The NGPC had to balance the competing interests of each factor to arrive at a decision. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.d.
8. 2013-04-11-IGO (Communiqué §1.g)	GAC reiterates its advice to the ICANN Board that appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch.	Dialogue	• The New gTLD Registry Agreement will require operators to provide appropriate preventative initial protection for the IGO identifiers. These protections will remain in place while the GAC, NGPC, ICANN Staff and community continue to actively work through outstanding implementation issues. • If the NGPC and GAC do not reach an agreement on outstanding implementation issues for protecting IGO names and acronyms by the first meeting of the NGPC following the ICANN 47 meeting in Durban, and subject to any matters that arise during the discussions, registry operators will be required to protect only the IGO names (and not the acronyms) identified on the GAC's IGO List. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
9. 2013-04-11-RAA (Communiqué §2)	The GAC advises the ICANN Board that the 2013 Registrar Accreditation Agreement should be finalized before any new gTLD contracts are approved.	Accept	• The Board approved the 2013 RAA at its 27 June 2013 Meeting. • The 2013 RAA requires all new gTLD registries to only use 2013 RAA registrars. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
10. 2013-04-11-WHOIS (Communiqué §3)	The GAC urges the ICANN Board to ensure that the GAC Principles Regarding gTLD WHOIS Services, approved in 2007, are duly taken into account by the recently established Directory Services Expert Working Group.	Accept	• The GAC Principles have been shared with the Expert Working Group. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
			• The NGPC accepted the GAC advice. • The Registry Agreement includes protection for an indefinite duration for

11. 2013-04-11-IOCRC (Communiqué §4)	The GAC advises the ICANN Board to amend the provisions in the new gTLD Registry Agreement pertaining to the IOC/RCRC names to confirm that the protections will be made permanent prior to the delegation of any new gTLDs.	Accept	IOC/RCRC names. Specification 5 of this version of the Registry Agreement includes a list of names (provided by the IOC and RCRC Movement) that "shall be withheld from registration or allocated to Registry Operator at the second level within the TLD." • This protection was added pursuant to a NGPC resolution to maintain these protections "until such time as a policy is adopted that may require further action" (204.11.26.NG03). • The resolution recognized the GNSO's initiation of an expedited PDP. Until such time as the GNSO approves recommendations in the PDP and the Board adopts them, the NGPC's resolutions protecting IOC/RCRC names will remain in place. • Should the GNSO submit any recommendations on this topic, the NGPC will confer with the GAC prior to taking action on any such recommendations. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
12. 2013-04-11-PIC SPEC (Communiqué §5, Annex 2)	The GAC requests more information on the Public Interest Commitments Specifications on the basis of the questions listed in annex II.	Provided	NGPC responses to the Annex 2 questions available at https://gacweb.icann.org/display/GACADV/2013-04-11-PICSPEC
13. 2013-04-11-Safeguards 1 (Communiqué Annex 1, 1)	1. WHOIS verification and checks — Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.	Accept	• ICANN (instead of Registry Operators) will implement the GAC's advice that checks identifying registrations in a gTLD with deliberately false, inaccurate or incomplete WHOIS data be conducted at least twice a year. • ICANN will perform a periodic sampling of WHOIS data across registries in an effort to identify potentially inaccurate records. • ICANN will also maintain statistical reports that identify the number of inaccurate WHOIS records identified. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
14. 2013-04-11-Safeguards 2 (Communiqué Annex	2. Mitigating abusive activity— Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets,		• A provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) obligates Registry Operators to include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or

1, 2)	phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.	Accept	otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
15. 2013-04-11-Safeguards 3 (Communiqué Annex 1, 3)	3. Security checks— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.	Accept	• A provision in the New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) requires Registry Operators periodically to conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. • The provision also requires Registry Operators to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate. • Because there are multiple ways for a Registry Operator to implement the required security checks, ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality. • The language included in Paragraph 3 of the attached PIC Specification provides the general guidelines for what Registry Operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks. This will permit Registry Operators to enter into agreements as soon as possible, while allowing for a careful and fulsome consideration by the community on the implementation details. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
16. 2013-04-11-Safeguards 4 ((Communiqué Annex 1, 4)	4. Documentation—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.	Accept	• As detailed in item 13 above, ICANN will maintain statistical reports that identify the number of inaccurate WHOIS records identified as part of the checks to identify registrations with deliberately false, inaccurate or incomplete WHOIS data. • As detailed in item 15 above, Registry Operators will be required to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. • Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.

17. 2013-04-11-Safeguards 5 ((Communiqué Annex 1, 5)	5. Making and Handling Complaints – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.	Accept	• Registry Operators are required to ensure that there is a mechanism for making complaints to the Registry Operator regarding malicious conduct in the TLD. • Section 4.1 of Specification 6 of the New gTLD Registry Agreement provides that, "Registry Operator shall provide to ICANN and publish 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." • Section 2.8 of the New gTLD Registry Agreement provides that a, "Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD." • ICANN operates the WHOIS Data Problem Reports System <http://www.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form>, which is a mechanism for making complaints that WHOIS information is inaccurate. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
18. 2013-04-11-Safeguards 6 (Communiqué Annex 1, 6)	6. Consequences – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.	Accept	• Consequences for the demonstrated provision of false WHOIS information are set forth in Section 3.7.7.2 of the 2013 RAA <http://www.icann.org/en/resources/registrars/raa/proposed-agreement-22apr13-en.pdf> [PDF, 311 KB]: "A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration." • Paragraph 1 of the PIC Specification includes a requirement that Registry Operator will use only ICANN accredited registrars that are party to the 2013 RAA so that these consequences are contractually required. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
19. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 1)	1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

20. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 2)	2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
21. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 3)	3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
22. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 4)	4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
23. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 5)	5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

24. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 6)	6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
25. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 7)	In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
26. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 8)	The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
27. 2013-04-11-Safeguards-Categories-2 (Communiqué Annex 1, Category 2, 1)	1. Restricted Access As an exception to the general rule that the gTLD domain name space is operated in an open manner registration may be restricted, in particular for strings mentioned under category 1 above. In these cases, the registration restrictions should be appropriate for the types of risks associated with the TLD. The registry operator should administer access in these kinds of registries in a transparent way that	Dialogue	• As noted above, the requested dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

	does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage.		
28. Safeguards-Categories-2 (Communiqué Annex 1, Category 2, 2)	2. **Exclusive Access** For strings representing generic terms, exclusive registry access should serve a public interest goal.	Accepted in part, dialogue on remainder	• For applicants seeking to impose exclusive registry access for "generic strings", the NGPC directed staff to defer moving forward with the contracting process for these applicants, pending a dialogue with the GAC. • The term "generic string" is defined to mean "a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others." • Exclusive registry access is defined as limiting registration of a generic string exclusively to a single person or entity and their affiliates. • For applicants not seeking to impose exclusive registry access, a provision in the in the New gTLD Registry Agreement requires TLDs to operate in a transparent manner consistent with general principles of openness and non-discrimination. • A PIC Specification also includes a provision to preclude registry operators from imposing eligibility criteria that limit registration of a generic string exclusively to a single person or entity and their "affiliates." • All applicants will be required to respond by a specified date indicating whether (a) the applicant is prepared to accept the proposed PIC Specification that precludes exclusive registry access or (b) the applicant is unwilling to accept the proposed PIC Specification because the applicant intends to implement exclusive registry access. • The NGPC will enter into a dialogue with the GAC to seek clarification on their advice with respect to exclusive registry access. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.c.

Announcements

Public Comment

For Journalists

Newsletter

Correspondence

Presentations

In Focus

Dashboard

RSS Feeds

RFPs

Litigation

Independent Review Process

Stay Connected

Your email address please.

News Alerts:	□ HTML	□ Plain Text
Newsletter:	□ HTML	□ Plain Text
Compliance Newsletter:	□ HTML	□ Plain Text
Policy Update:	□ HTML	□ Plain Text

Subscribe

Follow us @icann

Videos

Photos on Flickr

Facebook

ICANN Blog

Community Wiki

Planet ICANN

RSS Feeds

© 2013 Internet Corporation For Assigned Names and Numbers. Press | Site Map | Privacy Policy

Exhibit B

[Donuts Registry Agreement re "CAMERA”]

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 Atomic Maple, LLC, a Delaware limited liability company ("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 camera (the "TLD"). Upon the Effective Date and until the earlier of the expiration of the Term (as defined in Section 4.1) or the termination of this Agreement pursuant to Article 4, ICANN designates Registry Operator 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 duly organized, validly existing and in good standing under the laws of the jurisdiction set forth in the preamble hereto, and Registry Operator has all requisite power and authority and has obtained all necessary approvals to enter into and duly execute and deliver this Agreement; and

(iii) Registry Operator has delivered to ICANN a duly executed 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 thereto 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 has obtained all necessary corporate approvals to enter into and duly execute and deliver this Agreement.

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 2.1 in the Specification 6 attached hereto ("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 material modification to an Approved Service (each, an "Additional Service"), Registry Operator shall submit a request 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 in accordance with the bylaws of ICANN (as amended from time to time, the "ICANN Bylaws") applicable to Consensus Policies (the "RSEP"). Registry Operator may offer Additional Services only with the written approval of ICANN, and, upon any such approval, such Additional Services shall be deemed Registry Services under this Agreement. 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, which amendment shall be in a form reasonably acceptable to the parties.

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 the ICANN 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 in Specification 1 attached hereto ("Specification 1").

2.3 Data Escrow. Registry Operator shall comply with the registry data escrow procedures set forth in Specification 2 attached hereto ("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 set forth in Specification 3 attached hereto ("Specification 3").

2.5 Publication of Registration Data. Registry Operator shall provide public access to registration data in accordance with Specification 4 attached hereto ("Specification 4").

2.6 Reserved Names. Except to the extent that ICANN otherwise expressly authorizes in writing, Registry Operator shall comply with the requirements set forth in Specification 5 attached hereto ("Specification 5"). Registry Operator may at any time establish or modify policies concerning Registry Operator's ability to reserve (i.e., withhold from registration or allocate to Registry Operator, but not register to third parties, delegate, use, activate in the DNS or otherwise make available) or block additional character strings within the TLD at its discretion. Except as specified in Specification 5, if Registry Operator is the registrant for any domain names in the registry TLD, such registrations must be through an ICANN accredited registrar, and 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 Registry Interoperability and Continuity. Registry Operator shall comply with the Registry Interoperability and Continuity Specifications as set forth in Specification 6 attached hereto ("Specification 6").

2.8 Protection of Legal Rights of Third Parties. Registry Operator must specify, and comply with, the processes and procedures for launch of the TLD and initial registration-related and ongoing protection of the legal rights of third parties as set forth Specification 7 attached hereto ("Specification 7"). Registry Operator may, at its election, implement additional protections of the legal rights of third parties. Any changes or modifications to the process and procedures required by Specification 7 following the Effective Date must be approved in advance by ICANN in writing. Registry Operator must comply with all remedies imposed by ICANN pursuant to Section 2 of Specification 7, subject to Registry Operator's right to challenge such remedies as set forth in the applicable procedure described therein. Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.

2.9 Registrars.

(a) All domain name registrations in the TLD must be registered through an ICANN accredited registrar; provided, that Registry Operator need not use a registrar if it registers names in its own name in order to withhold such names from delegation or use in accordance with Section 2.6. Subject to the requirements of Specification 11, Registry Operator must provide non-discriminatory access to Registry Services to all ICANN accredited registrars that enter into and are in compliance with the registry-registrar agreement for the TLD; provided that Registry Operator may establish non-discriminatory criteria for qualification to register names in the TLD that are reasonably related to the proper functioning of the TLD. Registry Operator must use a uniform non-discriminatory agreement with all registrars authorized to register names in the TLD (the "Registry-Registrar Agreement"). Registry Operator may amend the Registry-Registrar Agreement from time to time; provided, however, that any material revisions thereto must be approved by ICANN before any such revisions become effective and binding on any registrar. Registry Operator will provide ICANN and all registrars authorized to register names in the TLD at least fifteen (15) calendar days written notice of any revisions to the Registry-Registrar Agreement before any such revisions become effective and binding on any registrar. During such period, ICANN will determine whether such proposed revisions are immaterial, potentially material or material in nature. If ICANN has not provided Registry Operator with notice of its determination within such fifteen (15) calendar-day period, ICANN shall be deemed to have determined that such proposed revisions are immaterial in nature. If ICANN determines, or is deemed to have determined under this Section 2.9(a), that such revisions are immaterial, then Registry Operator may adopt and implement such revisions. If ICANN determines such revisions are either material or potentially material, ICANN will thereafter follow its procedure regarding review and approval of changes to Registry-Registrar Agreements at <http://www.icann.org/en/resources/registries/rra-amendment-procedure>, and such revisions may not be adopted and implemented until approved by ICANN.

(b) If Registry Operator (i) becomes an Affiliate or reseller of an ICANN accredited registrar, or (ii) subcontracts the provision of any Registry Services to an ICANN accredited registrar, registrar reseller or any of their respective Affiliates, then, in either such case of (i) or (ii) above, Registry Operator will give ICANN prompt notice of the contract, transaction or other arrangement that resulted in such affiliation, reseller relationship or subcontract, as applicable, including, if requested by ICANN, copies of any contract relating thereto; provided, that ICANN will treat such contract or related documents that are appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15 (except that ICANN may disclose such contract and related documents to relevant competition authorities). ICANN reserves the right, but not the obligation, to refer any such contract, related documents, transaction or other arrangement to relevant competition authorities in the event that ICANN determines that such contract, related documents, transaction or other arrangement might raise significant competition issues under applicable law. If feasible and appropriate under the circumstances, ICANN will give Registry Operator advance notice prior to making any such referral to a competition authority.

(c) For the purposes of this Agreement: (i) "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, or in combination with one or more other persons or entities, controls, is controlled by, or is under common control with, the person or entity specified, and (ii) "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

2.10 Pricing for Registry Services.

(a) With respect to initial domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying or other programs which had the effect of reducing the price charged to registrars, unless such refunds, rebates, discounts, product tying or other programs are of a limited duration that is clearly and conspicuously disclosed to the registrar when offered) of no less than thirty (30) calendar days. Registry Operator shall offer registrars the option to obtain initial domain name registrations for periods of one (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(b) With respect to renewal of domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying, Qualified Marketing Programs or other programs which had the effect of reducing the price charged to registrars) of no less than one hundred eighty (180) calendar days. Notwithstanding the foregoing sentence, with respect to renewal of domain name registrations: (i) 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) for the period beginning on the Effective Date and ending twelve (12) months following the Effective Date, the initial price charged for registrations in the TLD, or (B) for subsequent periods, a price for which Registry Operator provided a notice pursuant to the first sentence of this Section 2.10(b) within the twelve (12) month period preceding the effective date of the proposed price increase; and (ii) Registry Operator need not provide notice of any price increase for the imposition of the Variable Registry-Level Fee set forth in Section 6.3. Registry Operator 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 (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(c) In addition, Registry Operator must have uniform pricing for renewals of domain name registrations ("Renewal Pricing"). For the purposes of determining Renewal Pricing, the price for each domain registration renewal must be identical to the price of all other domain name registration renewals in place at the time of such renewal, and such price must take into account universal application of any refunds, rebates, discounts, product tying or other programs in place at the time of renewal. The foregoing requirements of this Section 2.10(c) shall not apply for (i) purposes of determining Renewal Pricing if the registrar has provided Registry Operator with documentation that demonstrates that the applicable registrant expressly agreed in its registration agreement with registrar to higher Renewal Pricing at the time of the initial registration of the domain name following clear and conspicuous disclosure of such Renewal Pricing to such registrant, and (ii) discounted Renewal Pricing pursuant to a Qualified Marketing Program (as defined below). The parties acknowledge that the purpose of this Section 2.10(c) is to prohibit abusive and/or discriminatory Renewal Pricing practices imposed by Registry

Operator without the written consent of the applicable registrant at the time of the initial registration of the domain and this Section 2.10(c) will be interpreted broadly to prohibit such practices. For purposes of this Section 2.10(c), a "Qualified Marketing Program" is a marketing program pursuant to which Registry Operator offers discounted Renewal Pricing, provided that each of the following criteria is satisfied: (i) the program and related discounts are offered for a period of time not to exceed one hundred eighty (180) calendar days (with consecutive substantially similar programs aggregated for purposes of determining the number of calendar days of the program), (ii) all ICANN accredited registrars are provided the same opportunity to qualify for such discounted Renewal Pricing; and (iii) the intent or effect of the program is not to exclude any particular class(es) of registrations (e.g., registrations held by large corporations) or increase the renewal price of any particular class(es) of registrations. Nothing in this Section 2.10(c) shall limit Registry Operator's obligations pursuant to Section 2.10(b).

(d) Registry Operator shall provide public query-based DNS lookup service for the TLD (that is, operate the Registry TLD zone servers) at its sole expense.

2.11 Contractual and Operational Compliance Audits.

(a) ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct, contractual compliance audits to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. Such audits shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) 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, and (b) use commercially reasonable efforts to conduct such audit during regular business hours and in such a manner as to not unreasonably disrupt the operations of Registry Operator. As part of such audit and upon request by ICANN, Registry Operator shall timely provide all responsive documents, data and any other information reasonably necessary to demonstrate Registry Operator's compliance with this Agreement. Upon no less than ten (10) 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 representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. ICANN will treat any information obtained in connection with such audits that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15.

(b) Any audit conducted pursuant to Section 2.11(a) will be at ICANN's expense, unless (i) Registry Operator (A) controls, is controlled by, is under common control or is otherwise Affiliated with, any ICANN accredited registrar or registrar reseller or any of their respective Affiliates, or (B) has subcontracted the provision of Registry Services to an ICANN accredited registrar or registrar reseller or any of their respective Affiliates, and, in either case of (A) or (B) above, the audit relates to Registry Operator's compliance with Section 2.14, in which case Registry Operator shall reimburse ICANN for all reasonable costs and expenses associated with the portion of the audit related to Registry Operator's compliance with Section 2.14, or (ii) the audit is related to a discrepancy in the fees paid by Registry Operator hereunder in excess of 5% in a given quarter to ICANN's detriment, in which case Registry Operator shall reimburse ICANN for all reasonable costs and expenses associated with the entirety of such audit. In either such case of (i) or (ii) above, such 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.

(c) Notwithstanding Section 2.11(a), if Registry Operator is found not to be in compliance with its representations and warranties contained in Article 1 of this Agreement or its covenants contained in Article 2 of this Agreement in two consecutive audits conducted pursuant to this Section 2.11, ICANN may increase the number of such audits to one per calendar quarter.

(d) Registry Operator will give ICANN immediate notice of Registry Operator's knowledge of the commencement of any of the proceedings referenced in Section 4.3(d) or the occurrence of any of the matters specified in Section 4.3(f).

2.12 Continued Operations Instrument. Registry Operator shall comply with the terms and conditions relating to the Continued Operations Instrument set forth in Specification 8 attached hereto ("Specification 8").

2.13 Emergency Transition. Registry Operator agrees that, in the event that any of the emergency thresholds for registry functions set forth in Section 6 of Specification 10 is reached, ICANN may designate an emergency interim registry operator of the registry for the TLD (an "Emergency Operator") in accordance with ICANN's registry transition process (available at <http://www.icann.org/en/resources/registries/transition-processes>) (as the same may be amended from time to time, the "Registry Transition Process") until such time as Registry Operator has demonstrated to ICANN's reasonable satisfaction that it can resume operation of the registry for the TLD without the reoccurrence of such failure. Following such demonstration, Registry Operator may transition back into operation of the registry for the TLD pursuant to the procedures set out in the Registry Transition Process, provided that Registry Operator pays all reasonable costs incurred (i) by ICANN as a result of the designation of the Emergency Operator and (ii) by the Emergency Operator in connection with the operation of the registry for the TLD, which costs shall be documented in reasonable detail in records that shall be made available to Registry Operator. In the event ICANN designates an Emergency Operator pursuant to this Section 2.13 and the Registry Transition Process, Registry Operator shall provide ICANN or any such Emergency Operator with all data (including the 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 Emergency Operator. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event that an Emergency Operator is designated pursuant to this Section 2.13. In addition, in the event of such failure, ICANN shall retain and may enforce its rights under the Continued Operations Instrument.

2.14 Registry Code of Conduct. In connection with the operation of the registry for the TLD, Registry Operator shall comply with the Registry Code of Conduct as set forth in Specification 9 attached hereto ("Specification 9").

2.15 Cooperation with Economic Studies. If ICANN initiates or commissions an economic study on the impact or functioning of new generic top-level domains on the Internet, the DNS or related matters, Registry Operator shall reasonably cooperate with such study, including by delivering to ICANN or its designee conducting such study all data related to the operation of the TLD reasonably necessary for the purposes of such study requested by ICANN or its designee, provided, that Registry Operator may withhold (a) any internal analyses or evaluations prepared by Registry Operator with respect to such data and (b) any data to the extent that the delivery of such data would be in violation of applicable law. Any data delivered to ICANN or its designee pursuant to this Section 2.15 that is appropriately marked as confidential (as required by Section 7.15) shall be treated as Confidential Information of Registry Operator in accordance with Section 7.15, provided that, if ICANN aggregates and makes anonymous such data, ICANN or its designee may disclose such data to any third party. Following completion of an economic study for which Registry Operator has provided data, ICANN will destroy all data provided by Registry Operator that has not been aggregated and made anonymous.

2.16 Registry Performance Specifications. Registry Performance Specifications for operation of the TLD will be as set forth in Specification 10 attached hereto ("Specification 10"). Registry Operator shall comply with such Performance Specifications and, for a period of at least one (1) year, shall keep technical and operational records sufficient to evidence compliance with such specifications for each calendar year during the Term.

2.17 Additional Public Interest Commitments. Registry Operator shall comply with the public interest commitments set forth in Specification 11 attached hereto ("Specification 11").

2.18 Personal Data. Registry Operator shall (i) notify each ICANN-accredited registrar that is a party to the registry-registrar agreement for the TLD of the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to Registry Operator by such registrar is collected and used under this Agreement or otherwise and the intended recipients (or categories of recipients) of such Personal Data, and (ii) require such registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. Registry Operator shall take reasonable steps to protect Personal Data collected from such registrar from loss, misuse, unauthorized disclosure, alteration or destruction. Registry Operator shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

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.

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.

3.4 Root-zone Information Publication. ICANN's publication of root-zone contact information for the 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/.

3.5 Authoritative Root Database. To the extent that ICANN is authorized to set policy with regard to an authoritative root server system (the "Authoritative Root Server System"), ICANN shall use commercially reasonable efforts to (a) ensure that the authoritative root will point to the top-level domain nameservers designated by Registry Operator for the TLD, (b) maintain a stable, secure, and authoritative publicly available database of relevant information about the TLD, in accordance with ICANN publicly available policies and procedures, and (c) coordinate the Authoritative Root Server System so that it is operated and maintained in a stable and secure manner; provided, that ICANN shall not be in breach of this Agreement and ICANN shall have no liability in the event that any third party (including any governmental entity or internet service provider) blocks or restricts access to the TLD in any jurisdiction.

ARTICLE 4.

TERM AND TERMINATION

4.1 Term. The term of this Agreement will be ten (10) years from the Effective Date (as such term may be extended pursuant to Section 4.2, the "Term").

4.2 Renewal.

(a) This Agreement will be renewed for successive periods of ten (10) years upon the expiration of the initial Term set forth in Section 4.1 and each successive Term, unless:

(i) Following notice by ICANN to Registry Operator of a fundamental and material breach of Registry Operator's covenants set forth in Article 2 or breach of its payment obligations under Article 6 of this Agreement, which notice shall include with specificity the details of the alleged breach, and such breach has not been cured within thirty (30) calendar days of such notice, (A) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator has been in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (B) Registry Operator has failed 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 of competent jurisdiction; or

(ii) During the then current Term, Registry Operator shall have been found by an arbitrator (pursuant to Section 5.2 of this Agreement) or a court of competent jurisdiction on at least three (3) separate occasions to have been in (A) fundamental and material breach (whether or not cured) of Registry Operator's covenants set forth in Article 2 or (B) breach of its payment obligations under Article 6 of this Agreement.

(b) Upon the occurrence of the events set forth in Section 4.2(a) (i) or (ii), the Agreement shall terminate at the expiration of the then-current Term.

4.3 Termination by ICANN.

(a) ICANN may, upon notice to Registry Operator, terminate this Agreement if: (i) Registry Operator fails to cure (A) any fundamental and material breach of Registry Operator's representations and warranties set forth in Article 1 or covenants set forth in Article 2, or (B) any breach of Registry Operator's 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, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (iii) Registry Operator 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 of competent jurisdiction.

(b) ICANN may, upon notice to Registry Operator, terminate this Agreement if Registry Operator fails to complete all testing and procedures (identified by ICANN in writing to Registry Operator prior to the date hereof) for delegation of the TLD into the root zone within twelve (12) months of the Effective Date. Registry Operator may request an extension for up to additional twelve (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 (i) Registry Operator fails to cure a material 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, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in material breach of such covenant, and (iii) Registry Operator fails to cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(d) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator makes an assignment for the benefit of creditors or similar act, (ii) attachment, garnishment or similar proceedings are commenced against Registry Operator, which proceedings are a material threat to Registry Operator's ability to operate the registry for the TLD, and are not dismissed within sixty (60) calendar days of their commencement, (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registry Operator or maintains control over any of Registry Operator's property, (iv) execution is levied upon any material property of Registry Operator, (v) proceedings are instituted by or against Registry Operator under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within sixty (60) calendar days of their commencement, or (vi) Registry Operator files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101, et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations or the operation of the TLD.

(e) ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement pursuant to Section 2 of Specification 7 or Sections 2 and 3 of Specification 11, subject to Registry Operator's right to challenge such termination as set forth in the applicable procedure described therein.

(f) ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator knowingly employs any officer who is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) calendar days of Registry Operator's knowledge of the foregoing, or (ii) any member of Registry Operator's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registry Operator's board of directors or similar governing body within thirty (30) calendar days of Registry Operator's knowledge of the foregoing.

(g) ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement as specified in Section 7.5.

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 of competent jurisdiction has finally determined that ICANN is in fundamental and material breach of such covenants, 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 of competent jurisdiction.

(b) 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 pursuant to Section 4.1 or Section 4.2 or any termination of this Agreement pursuant to Section 4.3 or Section 4.4, Registry Operator shall provide ICANN or any successor registry operator that may be designated by ICANN for the TLD in accordance with this Section 4.5 with all data (including the 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 operator. After consultation with Registry Operator, ICANN shall determine whether or not to transition operation of the TLD to a successor registry operator in its sole discretion and in conformance with the Registry Transition Process; provided, however, that (i) ICANN will take into consideration any intellectual property rights of Registry Operator (as communicated to ICANN by Registry Operator) in determining whether to transition operation of the TLD to a successor registry operator and (ii) if Registry Operator demonstrates to ICANN's reasonable satisfaction that (A) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator or its Affiliates for their exclusive use, (B) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (C) transitioning operation of the TLD is not necessary to protect the public interest, then ICANN may not transition operation of the TLD to a successor registry operator upon the expiration or termination of this Agreement without the consent of Registry Operator (which shall not be unreasonably withheld, conditioned or delayed). For the avoidance of doubt, the foregoing sentence shall not prohibit ICANN from delegating the TLD pursuant to a future application process for the delegation of top-level domains, subject to any processes and objection procedures instituted by ICANN in connection with such application process intended to protect the rights of third parties. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event of a transition of the TLD pursuant to this Section 4.5. In addition, ICANN or its designee shall retain and may enforce its rights under the Continued Operations Instrument for the maintenance and operation of the TLD, regardless of the reason for termination or expiration of this Agreement.

4.6 Effect of Termination. Upon any expiration of the Term or termination of this Agreement, the obligations and rights of the parties hereto shall cease, provided that such 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, Article 7, Section 2.12, Section 4.5, and this Section 4.6 shall survive the expiration or termination of this Agreement. For the avoidance of doubt, the rights of Registry Operator to operate the registry for the TLD shall immediately cease upon any expiration of the Term or termination of this Agreement.

ARTICLE 5.

DISPUTE RESOLUTION

5.1 Mediation. In the event of any dispute arising under or in connection with this Agreement, before either party may initiate arbitration pursuant to Section 5.2 below, ICANN and Registry Operator must attempt to resolve the dispute through mediation in accordance with the following terms and conditions:

(a) A party shall submit a dispute to mediation by written notice to the other party. The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days of delivery of written notice pursuant to this Section 5.1, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 5.1(a).

(b) The mediator shall conduct the mediation in accordance with the rules and procedures that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute. The mediation shall be treated as a settlement discussion and shall therefore be confidential and may not be used against either party in any later proceeding relating to the dispute, including any arbitration pursuant to Section 5.2. The mediator may not testify for either party in any later proceeding relating to the dispute.

(c) Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator. Each party shall treat information received from the other party pursuant to the mediation that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of such other party in accordance with Section 7.15.

(d) If the parties have engaged in good faith participation in the mediation but have not resolved the dispute for any reason, either party or the mediator may terminate the mediation at any time and the dispute can then proceed to arbitration pursuant to Section 5.2 below. If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following the date of the notice delivered pursuant to Section 5.1(a), the mediation shall automatically terminate (unless extended by agreement of the parties) and the dispute can then proceed to arbitration pursuant to Section 5.2 below.

5.2 Arbitration. Disputes arising under or in connection with this Agreement that are not resolved pursuant to Section 5.1, 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. The arbitration will be conducted in the English language and will occur in Los Angeles County, California. Any arbitration will be in front of a single arbitrator, unless (i) ICANN is seeking punitive or exemplary damages, or operational sanctions, (ii) the parties agree in writing to a greater number of arbitrators, or (iii) the dispute arises under Section 7.6 or 7.7. In the case of clauses (i), (ii) or (iii) in the preceding sentence, the arbitration will be in front of three arbitrators with each party selecting one arbitrator and the two selected arbitrators selecting the third arbitrator. In order to expedite the arbitration and limit its cost, the arbitrator(s) shall establish page limits for the parties' filings in conjunction with the arbitration, and should the arbitrator(s) determine that a hearing is necessary, the hearing shall be limited to one (1) calendar day, provided that in any arbitration in which ICANN is seeking punitive or exemplary damages, or operational sanctions, the hearing may be extended for one (1) additional calendar day if agreed upon by the parties or ordered by the arbitrator(s) based on the arbitrator(s) independent determination or the reasonable request of one of the parties thereto. The prevailing party in the arbitration will have the right to recover its costs and reasonable attorneys' fees, which the arbitrator(s) shall include in the awards. In the event the arbitrators determine that Registry Operator has been repeatedly and willfully in fundamental and material breach of its obligations set forth in Article 2, Article 6 or Section 5.4 of this Agreement, ICANN may request the arbitrators award punitive or exemplary damages, or operational sanctions (including without limitation an order temporarily restricting Registry Operator's right to sell new registrations). Each party shall treat information received from the other party pursuant to the arbitration that is appropriately marked as confidential (as required by Section 7.15) as

Confidential Information of such other party in accordance with Section 7.15. 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; 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 an amount equal to the 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 breaches of this Agreement will be limited to an amount equal to the 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, except with respect to Registry Operator's indemnification obligations pursuant to Section 7.1 and Section 7.2. 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. Except as otherwise provided in this Agreement, neither party makes any warranty, express or implied, with respect to the services rendered by itself, its servants or agents, or the results obtained from their work, including, without limitation, any implied warranty of merchantability, non-infringement or fitness for a particular purpose.

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 or court of competent jurisdiction specific performance of the terms of this Agreement (in addition to any other remedy to which each party is entitled).

ARTICLE 6.

FEES

6.1 Registry-Level Fees.

(a) 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 (collectively, the "Registry-Level Fees"). 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 Transactions have occurred in the TLD during any calendar quarter or any consecutive four calendar quarter period in the aggregate (the "Transaction Threshold") and shall apply to each Transaction that occurred during each quarter in which the Transaction Threshold has been met, but shall not apply to each quarter in which the Transaction Threshold has not been met. Registry Operator's obligation to pay the quarterly registry-level fixed fee will begin on the date on which the TLD is delegated in the DNS to Registry Operator. The first quarterly payment of the registry-level fixed fee will be prorated based on the number of calendar days between the delegation date and the end of the calendar quarter in which the delegation date falls.

(b) Subject to Section 6.1(a), Registry Operator shall pay the Registry-Level Fees on a quarterly basis to an account designated by ICANN within thirty (30) calendar days following the date of the invoice provided 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 fourteen (14) calendar 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 (accounting, in the aggregate, for payment of two-thirds of all registrar-level fees (or such portion of ICANN accredited registrars necessary to approve variable accreditation fees under the then-current registrar accreditation agreement), 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 "Variable Registry-Level Fee"). 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 that are party to a registry-registrar agreement with Registry Operator (which agreement may specifically provide for the reimbursement of Variable Registry-Level Fees paid by Registry Operator pursuant to this Section 6.3); 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-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 Pass Through Fees. Registry Operator shall pay to ICANN (i) a one-time fee equal to US$5,000 for access to and use of the Trademark Clearinghouse as described in Specification 7 (the "RPM Access Fee") and (ii) an amount specified by ICANN not to exceed US$0.25 per Sunrise Registration and Claims Registration (as such terms are used in Trademark Clearinghouse RPMs incorporated herein pursuant to Specification 7) (the "RPM Registration Fee"). The RPM Access Fee will be invoiced as of the Effective Date of this Agreement, and Registry Operator shall pay such fee to an account specified by ICANN within thirty (30) calendar days following the date of the invoice. ICANN will invoice Registry Operator quarterly for the RPM Registration Fee, which shall be due in accordance with the invoicing and payment procedure specified in Section 6.1.

6.5 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 adjusted, at ICANN's discretion, by a percentage equal to the percentage change, 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 adjustment. Any fee adjustment under this Section 6.5 shall be effective as of the first day of the first calendar quarter following at least thirty (30) days after ICANN's delivery to Registry Operator of such fee adjustment notice.

6.6 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.

MISCELLANEOUS

7.1 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 reasonable legal fees and expenses, arising out of or relating to intellectual property ownership rights with respect to the TLD, the delegation of the TLD to Registry Operator, 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: (i) due to the actions or omissions of ICANN, its subcontractors, panelists or evaluators specifically related to and occurring during the registry TLD application process (other than actions or omissions requested by or for the benefit of Registry Operator), or (ii) due to a breach by ICANN of any obligation contained in this Agreement or any willful misconduct by ICANN. 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 of competent jurisdiction 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 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 are engaging in the same acts or omissions giving rise to such claim. For the purposes of reducing Registry Operator's liability under Section 7.1(a) pursuant to this Section 7.1(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 7.1(a) above, the number of domains under management by such registry operator(s) shall nonetheless be included in the calculation in the preceding sentence.

7.2 Indemnification Procedures. If any third-party claim is commenced that is indemnified under Section 7.1 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's policies, Bylaws 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 7.2, 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 and Registry Operator shall cooperate in such defense.

7.3 Defined Terms. For purposes of this Agreement, unless such definitions are amended pursuant to a Consensus Policy at a future date, in which case the following definitions shall be deemed amended and restated in their entirety as set forth in such Consensus Policy, 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.

7.4 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.

7.5 Change of Control; Assignment and Subcontracting. Except as set forth in this Section 7.5, neither party may assign any of its rights and obligations under this Agreement without the prior written approval of the other party, which approval will not be unreasonably withheld. For purposes of this Section 7.5, a direct or indirect change of control of Registry Operator or any subcontracting arrangement that relates to any Critical Function (as identified in Section 6 of Specification 10) for the TLD (a "Material Subcontracting Arrangement") shall be deemed an assignment.

(a) Registry Operator must provide no less than thirty (30) calendar days advance notice to ICANN of any assignment or Material Subcontracting Arrangement, and any agreement to assign or subcontract any portion of the operations of the TLD (whether or not a Material Subcontracting Arrangement) must mandate compliance with all covenants, obligations and agreements by Registry Operator hereunder, and Registry Operator shall continue to be bound by such covenants, obligations and agreements. Registry Operator must also provide no less than thirty (30) calendar days advance notice to ICANN prior to the consummation of any transaction anticipated to result in a direct or indirect change of control of Registry Operator.

(b) Within thirty (30) calendar days of either such notification pursuant to Section 7.5(a), ICANN may request additional information from Registry Operator establishing (i) compliance with this Agreement and (ii) that the party acquiring such control or entering into such assignment or Material Subcontracting Arrangement (in any case, the "Contracting Party") and the ultimate parent entity of the Contracting Party meets the ICANN-adopted specification or policy on registry operator criteria then in effect (including with respect to financial resources and operational and technical capabilities), in which case Registry Operator must supply the requested information within fifteen (15) calendar days.

(c) Registry Operator agrees that ICANN's consent to any assignment, change of control or Material Subcontracting Arrangement will also be subject to background checks on any proposed Contracting Party (and such Contracting Party's Affiliates).

(d) If ICANN fails to expressly provide or withhold its consent to any assignment, direct or indirect change of control of Registry Operator or any Material Subcontracting Arrangement within thirty (30) calendar days of ICANN's receipt of notice of such transaction (or, if ICANN has requested additional information from Registry Operator as set forth above, thirty (30) calendar days of the receipt of all requested written information regarding such transaction) from Registry Operator, ICANN shall be deemed to have consented to such transaction.

(e) In connection with any such assignment, change of control or Material Subcontracting Arrangement, Registry Operator shall comply with the Registry Transition Process.

(f) Notwithstanding the foregoing, (i) any consummated change of control shall not be voidable by ICANN; provided, however, that, if ICANN reasonably determines to withhold its consent to such transaction, ICANN may terminate this Agreement pursuant to Section 4.3(g), (ii) ICANN may assign this Agreement without the consent of Registry Operator upon approval of the ICANN Board of Directors in conjunction with a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (iii) Registry Operator may assign this Agreement without the consent of ICANN directly to a wholly-owned subsidiary of Registry Operator, or, if Registry Operator is a wholly-owned subsidiary, to its direct parent or to another wholly-owned subsidiary of its direct parent, upon such subsidiary's or parent's, as applicable, express assumption of the terms and conditions of this Agreement, and (iv) ICANN shall be deemed to have consented to any assignment, Material Subcontracting Arrangement or change of control transaction in which the Contracting Party is an existing operator of a generic top-level domain pursuant to a registry agreement between such Contracting Party and ICANN (provided that such Contracting Party is then in compliance with the terms and conditions of such registry agreement in all material respects), unless ICANN provides to Registry Operator a written objection to such transaction within ten (10) calendar days of ICANN's receipt of notice of such transaction pursuant to this Section 7.5. Notwithstanding Section 7.5(a), in the event an assignment is made pursuant to clauses (ii) or (iii) of this Section 7.5(f), the assigning party will provide the other party with prompt notice following any such assignment.

7.6 Amendments and Waivers.

(a) If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein) and all other registry agreements between ICANN and the Applicable Registry Operators (the "Applicable Registry Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 7.6; provided that a Special Amendment may not be a Restricted Amendment.

(b) Prior to submitting a Special Amendment for Registry Operator Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registry Operators in accordance with Section 7.9. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registry Operators).

(c) If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registry Operators. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable

Registry Operators, such Special Amendment receives Registry Operator Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registry Operators, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registry Operator (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registry Operator Approval, the Special Amendment shall be deemed not approved by the Applicable Registry Operators (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

(d) If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of Specification 1, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registry Operator shall comply with its obligations pursuant to Section 2.2 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 7.6(d), the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject matter of such Rejected Amendment was the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

(e) If (a) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of Specification 1, (b) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (c) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (A) recommends adoption of the Rejected Amendment as Consensus Policy or (B) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

(i) the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

(ii) the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

(iii) to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registry Operators, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

(iv) the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

(v) following such public comment period, the ICANN Board of Directors must (a) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty (60) calendar days; and (b) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registry Operator Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 7.6(f), be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registry Operator (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registry fees charged by ICANN hereunder, or amend this Section 7.6.

(f) Notwithstanding the provisions of Section 7.6(e), a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registry Operators, submits to the ICANN Board of Directors an alternative to the Board Amendment (an "Alternative Amendment") that meets the following requirements:

(i) sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

(ii) addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

(iii) compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registry Operators, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses (i) through (iii) in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registry Operator Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registry Operator, which effective date shall deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registry Operator Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registry Operator Approval within thirty (30) calendar days of submission of such Alternative Amendment to the Applicable Registry Operators (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registry Operator (which effective date shall deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 7.6(f)(i) through 7.6(f)(iii). The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 7.6(e)(i) through 7.6(e)(v).

(g) In the event that Registry Operator believes an Approved Amendment does not meet the substantive requirements set out in this Section 7.6 or has been adopted in contravention of any of the procedural provisions of this Section 7.6, Registry Operator may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Article 5, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registry Operator of the Approved Amendment, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

(h) Registry Operator may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registry Operator hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registry Operator of such Approved Amendment. Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registry Operator. An Exemption Request may only be granted upon a clear and convincing showing by Registry Operator that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registry Operator. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants. Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement. If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registry Operator may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Article 5. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registry Operator that are approved by ICANN pursuant to this Section 7.6(j), agreed to by ICANN following mediation pursuant to Section 5.1 or through an arbitration decision pursuant to Section 5.2 shall exempt Registry Operator from any Approved Amendment, and no Exemption Request granted to any other Applicable Registry Operator (whether by ICANN or through arbitration) shall have any effect under this Agreement or exempt Registry Operator from any Approved Amendment.

(i) Except as set forth in this Section 7.6, Section 7.7 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 7.6 or Section 7.7 shall restrict ICANN and Registry Operator from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall 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 shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Sections 7.6 or 7.7 shall be deemed to limit Registry Operator's obligation to comply with Section 2.2.

(j) For purposes of this Section 7.6, the following terms shall have the following meanings:

(i) "Applicable Registry Operators" means, collectively, the registry operators of top-level domains party to a registry agreement that contains a provision similar to this Section 7.6, including Registry Operator.

(ii) "Registry Operator Approval" means the receipt of each of the following: (A) the affirmative approval of the Applicable Registry Operators whose payments to ICANN accounted for two-thirds of the total amount of fees (converted to U.S. dollars, if applicable, at the prevailing exchange rate published the prior day in the U.S. Edition of the Wall Street Journal for the date such calculation is made by ICANN) paid to ICANN by all the Applicable Registry Operators during the immediately previous calendar year pursuant to the Applicable Registry Agreements, and (B) the affirmative approval of a majority of the Applicable Registry Operators at the time such approval is obtained. For the avoidance of doubt, with respect to clause (B), each Applicable Registry Operator shall have one vote for each top-level domain operated by such Registry Operator pursuant to an Applicable Registry Agreement.

(iii) "Restricted Amendment" means the following: (A) an amendment of Specification 1, (B) except to the extent addressed in Section

2.10 hereof, an amendment that specifies the price charged by Registry Operator to registrars for domain name registrations, (C) an amendment to the definition of Registry Services as set forth in the first paragraph of Section 2.1 of Specification 6, or (D) an amendment to the length of the Term.

(iv) "Substantial and Compelling Reason in the Public Interest" means a reason that is justified by an important, specific, and articulated public interest goal that is within ICANN's mission and consistent with a balanced application of ICANN's core values as defined in ICANN's Bylaws.

(v) "Working Group" means representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)).

(k) Notwithstanding anything in this Section 7.6 to the contrary, (i) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for Approved Amendment to become effective with respect to Registry Operator, and (ii) no Approved Amendment adopted pursuant to Section 7.6 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.7 Negotiation Process.

(a) If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registry Stakeholder Group ("Chair") desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a "Negotiation Notice"). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.7 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve (12) month period beginning on July 1, 2014.

(b) Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group (as defined in Section 7.6) shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the "Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the "Discussion Period").

(c) If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed

Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval (as defined in Section 7.6) and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(d) If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

(i) The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, who has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.7(d)(i).

(ii) The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

(iii) Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

(iv) If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(v) If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.7(e)(ii) below.

(e) If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.2, subject to the requirements and limitations of this Section 7.7(e).

(i) If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, the Working Group or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators), and information regarding such comments and consideration shall be provided to a three (3) person arbitrator panel. Each party may modify its Proposed Revisions before and after the Posting Period. The arbitration proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. Except as set forth in this Section 7.7, the arbitration shall be conducted pursuant to Section 5.2.

(ii) No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed

Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of Specification 1, or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Articles 1, 3 and 6; Sections 2.1, 2.2, 2.5, 2.7, 2.9, 2.10, 2.16, 2.17, 2.19, 4.1, 4.2, 7.3, 7.6, 7.7, 7.8, 7.10, 7.11, 7.12, 7.13, 7.14, 7.16; Section 2.8 and Specification 7 (but only to the extent such Proposed Revisions seek to implement an RPM not contemplated by Sections 2.8 and Specification 7); Exhibit A; and Specifications 1, 4, 6, 10 and 11.

(iii) The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

(iv) No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registry Operator Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

(v) In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registry Operators and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator and deemed an Approved Amendment hereunder.

(f) With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registry may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 7.6.

(g) Notwithstanding anything in this Section 7.7 to the contrary, (a) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registry Operator, and (b) no Approved Amendment adopted pursuant to Section 7.7 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.8 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.

7.9 General Notices. Except for notices pursuant to Sections 7.6 and 7.7, 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 Sections 7.6 and 7.7 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. Other than notices under Sections 7.6 or 7.7, 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 three (3) calendar days. Any notice required by Sections 7.6 or 7.7 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 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
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA
Telephone: +1-310-301-5800
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:
Atomic Maple, LLC
c/o Donuts Inc.
Contact Information Redacted

Telephone: Contact nformation Redacted
Facsimile: Contact nformation Redacted
Attention: Jonathon Nevett, Executive Vice President
Email: Contact n ormation Redacted

7.10 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.

7.11 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.

7.12 Ownership Rights. Nothing contained in this Agreement shall be construed as (a) establishing or granting to Registry Operator any property ownership rights or interests of Registry Operator in the TLD or the letters, words, symbols or other characters making up the TLD string, or (b) affecting any existing intellectual property or ownership rights of Registry Operator.

7.13 Severability; Conflicts with Laws. This Agreement shall be deemed severable; the invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of the balance of this Agreement or of any other term hereof, which shall remain in full force and effect. If any of the provisions hereof are determined to be invalid or unenforceable, the parties shall negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible. ICANN and the Working Group will mutually cooperate to develop an ICANN procedure for ICANN's review and consideration of alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement. Until such procedure is developed and implemented by ICANN, ICANN will review and consider alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement in a manner similar to ICANN's Procedure For Handling WHOIS Conflicts with Privacy Law.

7.14 Court Orders. ICANN will respect any order from a court of competent jurisdiction, including any orders from any jurisdiction where the consent or non-objection of the government was a requirement for the delegation of the TLD. Notwithstanding any other provision of this Agreement, ICANN's implementation of any such order will not be a breach of this Agreement

7.15 Confidentiality

(a) Subject to Section 7.15(c), during the Term and for a period of three (3) years thereafter, each party shall, and shall cause its and its Affiliates' officers, directors, employees and agents to, keep confidential and not publish or otherwise disclose to any third party, directly or indirectly, any information that is, and the disclosing party has marked as, or has otherwise designated in writing to the receiving party as, “confidential trade secret,” “confidential commercial information” or “confidential financial information” (collectively, “Confidential Information”), except to the extent such disclosure is permitted by the terms of this Agreement.

(b) The confidentiality obligations under Section 7.15(a) shall not apply to any Confidential Information that (i) is or hereafter becomes part of the public domain by public use, publication, general knowledge or the like through no fault of the receiving party in breach of this Agreement, (ii) can be demonstrated by documentation or other competent proof to have been in the receiving party’s possession prior to disclosure by the disclosing party without any obligation of confidentiality with respect to such information, (iii) is subsequently received by the receiving party from a third party who is not bound by any obligation of confidentiality with respect to such information, (iv) has been published by a third party or otherwise enters the public domain through no fault of the receiving party, or (v) can be demonstrated by documentation or other competent evidence to have been independently developed by or for the receiving party without reference to the disclosing party’s Confidential Information.

(c) Each party shall have the right to disclose Confidential Information to the extent that such disclosure is (i) made in response to a valid order of a court of competent jurisdiction or, if in the reasonable opinion of the receiving party’s legal counsel, such disclosure is otherwise required by applicable law; provided, however, that the receiving party shall first have given notice to the disclosing party and given the disclosing party a reasonable opportunity to quash such order or to obtain a protective order or confidential treatment order requiring that the Confidential Information that is the subject of such order or other applicable law be held in confidence by such court or other third party recipient, unless the receiving party is not permitted to provide such notice under such order or applicable law, or (ii) made by the receiving party or any of its Affiliates to its or their attorneys, auditors, advisors, consultants, contractors or other third parties for use by such person or entity as may be necessary or useful in connection with the performance of the activities under this Agreement, provided that such third party is bound by confidentiality obligations at least as stringent as those set forth herein, either by written agreement or through professional responsibility standards.

* * * * *

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: ______________________________
Akram Atallah
President, Generic Domains Division

ATOMIC MAPLE, LLC

By: ______________________________
Paul Stahura
President and CEO

EXHIBIT A

Approved Services

The ICANN gTLD Applicant Guidebook (located at http://newgtlds.icann.org/en/applicants/agb) and the RSEP specify processes for consideration of proposed registry services. Registry Operator may provide any service that is required by the terms of this Agreement. In addition, the following services (if any) are specifically identified as having been approved by ICANN prior to the effective date of the Agreement, and Registry Operator may provide such services:

1. DNS Service – TLD Zone Contents

Notwithstanding anything else in this Agreement, as indicated in section 2.2.3.3 of the gTLD Applicant Guidebook, permissible contents for the TLD's zone are:

1.1. Apex SOA record

1.2. Apex NS records and in-bailiwick glue for the TLD's DNS servers

1.3. NS records and in-bailiwick glue for DNS servers of registered names in the TLD

1.4. DS records for registered names in the TLD

1.5. Records associated with signing the TLD zone (i.e., RRSIG, DNSKEY, NSEC, and NSEC3)

(Note: The above language effectively does not allow, among other things, the inclusion of DNS resource records that would enable a dotless domain name (e.g., apex A, AAAA, MX records) in the TLD zone.)

If Registry Operator wishes to place any DNS resource record type into its TLD DNS zone (other than those listed in Sections 1.1 through 1.5 above), it must describe in detail its proposal and submit a Registry Services Evaluation Process (RSEP) request. This will be evaluated per RSEP to determine whether the service would create a risk of a meaningful adverse impact on security or stability of the DNS. Registry Operator recognizes and acknowledges that a service based on the use of less-common DNS resource records in the TLD zone, even if approved, might not work as intended for all users due to lack of software support.

2. Internationalized Domain Names (IDNs)

Registry Operator may offer registration of IDNs at the second and lower levels provided that Registry Operator complies with the following requirements:

2.1. Registry Operator must offer Registrars support for handling IDN registrations in EPP.

2.2. Registry Operator must handle variant IDNs as follows:

2.2.1. Variant IDNs (as defined in the Registry Operator's IDN tables and IDN Registration Rules) will be blocked from registration.

2.3. Registry Operator may offer registration of IDNs in the following languages/scripts (IDN Tables and IDN Registration Rules will be published by the Registry Operator as specified in the ICANN IDN Implementation Guidelines):

2.3.1. French Language

2.3.2. Spanish Language

3. Searchable Whois

Notwithstanding anything else in this Agreement, Registry Operator must offer a searchable Whois service compliant with the requirements described in Section 1.10 of Specification 4 of this Agreement. Registry Operator must make available the services only to authenticated users after they logged in by supplying proper credentials (i.e., user name and password). Registry Operator must issue such credentials exclusively to eligible users and institutions that supply sufficient proof of their legitimate interest in this feature (e.g., law enforcement agencies).

4. Specification 11 Registry Services

The following are descriptions of the Registry Services listed in Specification 11:

4.1. Domains Protected Marks List (DPML)

The DPML is a service that allows trademark rights holders to block certain labels from registration across multiple TLDs operated by the Registry Operator. The blocked names must comply with the provisions described in Specification 5, Section 3.3 of the Registry Agreement. Domain Names blocked by the DPML service will be either an exact match of a label or will contain an exact match of such labels, or may include domain names that are a misspelling or contain a misspelling of a label. Blocked labels do not prevent other trademark rights holders from unblocking the label and registering the domain name.

4.2. Claims Plus

Claims Plus is a service that provides notice to Registrars that a domain name they are trying to register matches a trademark registered in a trademark database used by the Registry Operator.

SPECIFICATION 1

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. **<u>Consensus Policies</u>**.

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 Specification. 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;

1.2.5 resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or

1.2.6 restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated.

1.3. Such categories of issues referred to in Section 1.2 of this Specification 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 ninety (90) calendar days, the Board shall reaffirm its temporary adoption every ninety (90) calendar days for a total period not to exceed one (1) year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one (1) year period expires or, if during such one (1) 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

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. **Deposits**. There will be two types of Deposits: Full and Differential. For both types, the universe of Registry objects to be considered for data escrow are those objects necessary in order to offer all of the approved Registry Services.

   1.1. "**Full Deposit**" will consist of data that reflects the state of the registry as of 00:00:00 UTC (Coordinated Universal Time) on the day that such Full Deposit is submitted to Escrow Agent.

   1.2. "**Differential Deposit**" means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database transactions since the previous Deposit was completed as of 00:00:00 UTC of each day, but Sunday. Differential Deposits must include complete Escrow Records as specified below that were not included or changed since the most recent full or Differential Deposit (i.e., newly added or modified domain names).

2. **Schedule for Deposits**. Registry Operator will submit a set of escrow files on a daily basis as follows:

   2.1. Each Sunday, a Full Deposit must be submitted to the Escrow Agent by 23:59 UTC.

   2.2. The other six (6) days of the week, a Full Deposit or the corresponding Differential Deposit must be submitted to Escrow Agent by 23:59 UTC.

3. **Escrow Format Specification**.

   3.1. **Deposit's Format**. Registry objects, such as domains, contacts, name servers, registrars, etc. will be compiled into a file constructed as described in draft-arias-noguchi-registry-data-escrow, see Part A, Section 9, reference 1 of this Specification and draft-arias-noguchi-dnrd-objects-mapping, see Part A, Section 9, reference 2 of this Specification (collectively, the "DNDE Specification"). The DNDE Specification describes some elements as optional; Registry Operator will include those elements in the Deposits if they are available. If not already an RFC, Registry Operator will use the most recent draft version of the DNDE Specification available at the Effective Date. Registry Operator may at its election use newer versions of the DNDE Specification after the Effective Date. Once the DNDE Specification is published as an RFC, Registry Operator will implement that version of the DNDE Specification, no later than one hundred eighty (180) calendar days after. UTF-8 character encoding will be used.

3.2. **Extensions**. If a Registry Operator offers additional Registry Services that require submission of additional data, not included above, additional "extension schemas" shall be defined in a case by case basis to represent that data. These "extension schemas" will be specified as described in Part A, Section 9, reference 2 of this Specification. Data related to the "extensions schemas" will be included in the deposit file described in Part A, Section 3.1 of this Specification. ICANN and the respective Registry Operator shall work together to agree on such new objects' data escrow specifications.

4. **Processing of Deposit files**. The use of compression is recommended in order to reduce electronic data transfer times, and storage capacity requirements. Data encryption will be used to ensure the privacy of registry escrow data. Files processed for compression and encryption will be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see Part A, Section 9, reference 3 of this Specification. 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, see Part A, Section 9, reference 4 of this Specification, that are also royalty-free. The process to follow for the data file in original text format is:

(1) The XML file of the deposit as described in Part A, Section 9, reference 1 of this Specification must be named as the containing file as specified in Section 5 but with the extension xml.

(2) The data file(s) are aggregated in a tarball file named the same as (1) but with extension tar.

(3) A compressed and encrypted OpenPGP Message is created using the tarball file as sole input. The suggested algorithm for compression is ZIP as per RFC 4880. The compressed data will 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.

(4) The file may be split as necessary if, once compressed and encrypted, it is larger than the file size limit agreed with the escrow agent. Every part of a

split file, or the whole file if not split, will be called a processed file in this section.

(5) A digital signature file will be generated for every processed file using the Registry Operator's private key. The digital signature file will be in binary OpenPGP format as per RFC 4880 Section 9, reference 3, and will not be compressed or encrypted. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.

(6) The processed files and digital signature files will then be transferred to the Escrow Agent through secure electronic mechanisms, such as, SFTP, SCP, HTTPS file upload, etc. as agreed between the Escrow Agent and the Registry Operator. Non-electronic delivery through a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices may be used if authorized by ICANN.

(7) The Escrow Agent will then validate every (processed) transferred data file using the procedure described in Part A, Section 8 of this Specification.

5. **File Naming Conventions**. Files will be named according to the following convention: {gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext} where:

5.1. {gTLD} is replaced with the gTLD name; in case of an IDN-TLD, the ASCII-compatible form (A-Label) must be used;

5.2. {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";

5.3. {type} is replaced by:

(1) "full", if the data represents a Full Deposit;

(2) "diff", if the data represents a Differential Deposit;

(3) "thin", if the data represents a Bulk Registration Data Access file, as specified in Section 3 of Specification 4;

5.4. {#} 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".

5.5. {rev} is replaced by the number of revision (or resend) of the file beginning with "0":

5.6. {ext} is replaced by "sig" if it is a digital signature file of the quasi-homonymous file. Otherwise it is replaced by "ryde".

6. **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 Operator and ICANN will exchange public keys by the same procedure.

7. **Notification of Deposits**. Along with the delivery of each Deposit, Registry Operator will deliver to Escrow Agent and to ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification (the "Interface Specification")) 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. Registry Operator will include the Deposit's "id" and "resend" attributes in its statement. The attributes are explained in Part A, Section 9, reference 1 of this Specification.

If not already an RFC, Registry Operator will use the most recent draft version of the Interface Specification at the Effective Date. Registry Operator may at its election use newer versions of the Interface Specification after the Effective Date. Once the Interface Specification is published as an RFC, Registry Operator will implement that version of the Interface Specification, no later than one hundred eighty (180) calendar days after such publishing.

8. **Verification Procedure**.

(1) The signature file of each processed file is validated.

(2) If processed files are pieces of a bigger file, the latter is put together.

(3) Each file obtained in the previous step is then decrypted and uncompressed.

(4) Each data file contained in the previous step is then validated against the format defined in Part A, Section 9, reference 1 of this Specification.

(5) If Part A, Section 9, reference 1 of this Specification includes a verification process, that will be applied at this step.

If any discrepancy is found in any of the steps, the Deposit will be considered incomplete.

9. **References**.

(1) Domain Name Data Escrow Specification (work in progress), http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow

(2) Domain Name Registration Data (DNRD) Objects Mapping, http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping

(3) OpenPGP Message Format, http://www.rfc-editor.org/rfc/rfc4880.txt

(4) OpenPGP parameters, http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml

(5) ICANN interfaces for registries and data escrow agents, http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces

PART B – LEGAL REQUIREMENTS

1. **Escrow Agent**. Prior to entering into an escrow agreement, the Registry Operator must provide notice to 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 amendments thereto. In addition, prior to entering into an escrow agreement, Registry Operator must obtain the consent of ICANN to (a) use the specified Escrow Agent, and (b) enter into the form of escrow agreement provided. ICANN must be expressly designated as a third-party beneficiary of the escrow agreement. ICANN reserves the right to withhold its consent to any Escrow Agent, escrow agreement, or any amendment thereto, all in its sole discretion.

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 fifteen (15) calendar 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 to ICANN or to a party designated in writing by ICANN on a non-exclusive, perpetual, irrevocable, royalty-free, paid-up basis, for any use related to the operation, maintenance or transition of the TLD.

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, (ii) protect the integrity and confidentiality of the Deposits using commercially reasonable measures and (iii) keep and safeguard each Deposit for one (1) year. 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. Registry Operator and ICANN will be provided with the right to designate a third-party auditor to audit Escrow Agent's compliance with the technical specifications and maintenance requirements of this Specification 2 from time to time.

   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.

6. **Release of Deposits**. Escrow Agent will make available for electronic download (unless otherwise requested) to ICANN or its designee, within twenty-four (24) hours, 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 has not received a notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent within five (5) calendar days after the Deposit's scheduled delivery date; (a) ICANN gave notice to Escrow Agent and Registry Operator of that failure; and (b) ICANN has not, within seven (7) calendar days after such notice, received the notification from Escrow Agent; or

6.3. ICANN has received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of failed verification of the latest escrow deposit for a specific date or a notification of a missing deposit, and the notification is for a deposit that should have been made on Sunday (i.e., a Full Deposit); (a) ICANN gave notice to Registry Operator of that receipt; and (b) ICANN has not, within seven (7) calendar days after such notice, received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of verification of a remediated version of such Full Deposit; or

6.4. ICANN has received five notifications from Escrow Agent within the last thirty (30) calendar days notifying ICANN of either missing or failed escrow deposits that should have been made Monday through Saturday (i.e., a Differential Deposit), and (x) ICANN provided notice to Registry Operator of the receipt of such notifications; and (y) ICANN has not, within seven (7) calendar days after delivery of such notice to Registry Operator, received notification from Escrow Agent of verification of a remediated version of such Differential Deposit; or

6.5. 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

6.6. Registry Operator has experienced a failure of critical registry functions and ICANN has asserted its rights pursuant to Section 2.13 of the Agreement; or

6.7. a competent court, arbitral, legislative, or government agency mandates the release of the Deposits to ICANN; or

6.8. pursuant to Contractual and Operational Compliance Audits as specified under Section 2.11 of the Agreement.

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 expiration or termination of the Registry Agreement or the Escrow Agreement.

7. **Verification of Deposits**.

7.1. Within twenty-four (24) hours after receiving each Deposit or corrected Deposit, Escrow Agent must verify the format and completeness of each Deposit and deliver to ICANN a notification generated for each Deposit. Reports will be delivered electronically using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification.

7.2. If Escrow Agent discovers that any Deposit fails the verification procedures or if Escrow Agent does not receive any scheduled Deposit, Escrow Agent must notify Registry Operator either by email, fax or phone and ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification) of such nonconformity or non-receipt within twenty-four (24) hours after receiving the non-conformant Deposit or the deadline for such Deposit, as applicable. Upon notification of such verification or delivery failure, Registry Operator must begin developing modifications, updates, corrections, and other fixes of the Deposit necessary for the Deposit to be delivered and pass the verification procedures and deliver such fixes to Escrow Agent as promptly as possible.

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**. 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 one set of monthly reports per gTLD, using the API described in draft-lozano-icann-registry-interfaces, see Specification 2, Part A, Section 9, reference 5, with the following content.

ICANN may request in the future that the reports be delivered by other means and using other formats. ICANN will use reasonable commercial efforts to preserve the confidentiality of the information reported until three (3) months after the end of the month to which the reports relate. Unless set forth in this Specification 3, any reference to a specific time refers to Coordinated Universal Time (UTC). Monthly reports shall consist of data that reflects the state of the registry at the end of the month (UTC).

1. **Per-Registrar Transactions Report**. This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD-transactions-yyyymm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyymm" is the year and month being reported. The file shall contain the following fields per registrar:

Field #	Field name	Description
01	registrar-name	Registrar's full corporate name as registered with IANA
02	iana-id	For cases where the registry operator acts as registrar (i.e., without the use of an ICANN accredited registrar) 9999 should be used, otherwise the sponsoring Registrar IANA id should be used as specified in http://www.iana.org/assignments/registrar-ids
03	total-domains	total domain names under sponsorship in any EPP status but pendingCreate that have not been purged
04	total-nameservers	total name servers (either host objects or name server hosts as domain name attributes) associated with domain names registered for the TLD in any EPP status but pendingCreate that have not been purged
05	net-adds-1-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of one (1) year (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
06	net-adds-2-yr	number of domains successfully registered (i.e., not

		in EPP pendingCreate status) with an initial term of two(2) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
07	net-adds-3-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of three (3) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
08	net-adds-4-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of four (4) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
09	net-adds-5-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of five (5) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
10	net-adds-6-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of six (6) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
11	net-adds-7-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of seven (7) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
12	net-adds-8-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of eight (8) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
13	net-adds-9-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of nine (9) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
14	net-adds-10-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of ten (10) years (and not deleted within the add grace period). A transaction must be reported in the month

		the add grace period ends.
15	net-renews-1-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of one (1) year (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
16	net-renews-2-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of two (2) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
17	net-renews-3-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of three (3) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
18	net-renews-4-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of four (4) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
19	net-renews-5-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of five (5) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
20	net-renews-6-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of six (6) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.

21	net-renews-7-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of seven (7) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
22	net-renews-8-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of eight (8) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
23	net-renews-9-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of nine (9) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
24	net-renews-10-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of ten (10) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
25	transfer-gaining-successful	number of domain transfers initiated by this registrar that were successfully completed (either explicitly or automatically approved) and not deleted within the transfer grace period. A transaction must be reported in the month the transfer grace period ends.
26	transfer-gaining-nacked	number of domain transfers initiated by this registrar that were rejected (e.g., EPP transfer op="reject") by the other registrar
27	transfer-losing-successfully	number of domain transfers initiated by another registrar that were successfully completed (either explicitly or automatically approved)
28	transfer-losing-nacked	number of domain transfers initiated by another registrar that this registrar rejected (e.g., EPP transfer op="reject")

29	transfer-disputed-won	number of transfer disputes in which this registrar prevailed (reported in the month where the determination happened)
30	transfer-disputed-lost	number of transfer disputes this registrar lost (reported in the month where the determination happened)
31	transfer-disputed-nodecision	number of transfer disputes involving this registrar with a split or no decision (reported in the month where the determination happened)
32	deleted-domains-grace	domains deleted within the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
33	deleted-domains-nograce	domains deleted outside the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
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-domains	total number of names affected by granted AGP (add grace period) exemption requests
39	attempted-adds	number of attempted (both successful and failed) domain name create commands

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 shall 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 in that line. No other lines besides the ones described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

2. **Registry Functions Activity Report**. This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD-activity-yyyymm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyymm" is the year and month being reported. The file shall contain the following fields:

Field #	Field Name	Description
01	operational-registrars	number of operational registrars at the end of the reporting period
02	ramp-up-registrars	number of registrars that have received a password for access to OT&E at the end of the reporting period
03	pre-ramp-up-registrars	number of registrars that have requested access, but have not yet entered the ramp-up period at the end of the reporting period
04	zfa-passwords	number of active zone file access passwords at the end of the reporting period
05	whois-43-queries	number of WHOIS (port-43) queries responded during the reporting period
06	web-whois-queries	number of Web-based Whois queries responded during the reporting period, not including searchable Whois
07	searchable-whois-queries	number of searchable Whois queries responded during the reporting period, if offered
08	dns-udp-queries-received	number of DNS queries received over UDP transport during the reporting period
09	dns-udp-queries-responded	number of DNS queries received over UDP transport that were responded during the reporting period
10	dns-tcp-queries-received	number of DNS queries received over TCP transport during the reporting period
11	dns-tcp-queries-responded	number of DNS queries received over TCP transport that were responded during the reporting period
12	srs-dom-check	number of SRS (EPP and any other interface) domain name "check" requests responded during the reporting period
13	srs-dom-create	number of SRS (EPP and any other interface) domain name "create" requests responded during the reporting period
14	srs-dom-delete	number of SRS (EPP and any other interface) domain name "delete" requests responded during the reporting period
15	srs-dom-info	number of SRS (EPP and any other interface) domain name "info" requests responded during the reporting period

Field #	Field Name	Description
16	srs-dom-renew	number of SRS (EPP and any other interface) domain name “renew” requests responded during the reporting period
17	srs-dom-rgp-restore-report	number of SRS (EPP and any other interface) domain name RGP “restore” requests delivering a restore report responded during the reporting period
18	srs-dom-rgp-restore-request	number of SRS (EPP and any other interface) domain name RGP “restore” requests responded during the reporting period
19	srs-dom-transfer-approve	number of SRS (EPP and any other interface) domain name “transfer” requests to approve transfers responded during the reporting period
20	srs-dom-transfer-cancel	number of SRS (EPP and any other interface) domain name “transfer” requests to cancel transfers responded during the reporting period
21	srs-dom-transfer-query	number of SRS (EPP and any other interface) domain name “transfer” requests to query about a transfer responded during the reporting period
22	srs-dom-transfer-reject	number of SRS (EPP and any other interface) domain name “transfer” requests to reject transfers responded during the reporting period
23	srs-dom-transfer-request	number of SRS (EPP and any other interface) domain name “transfer” requests to request transfers responded during the reporting period
24	srs-dom-update	number of SRS (EPP and any other interface) domain name “update” requests (not including RGP restore requests) responded during the reporting period
25	srs-host-check	number of SRS (EPP and any other interface) host “check” requests responded during the reporting period
26	srs-host-create	number of SRS (EPP and any other interface) host “create” requests responded during the reporting period
27	srs-host-delete	number of SRS (EPP and any other interface) host “delete” requests responded during the reporting period

Field #	Field Name	Description
28	srs-host-info	number of SRS (EPP and any other interface) host “info” requests responded during the reporting period
29	srs-host-update	number of SRS (EPP and any other interface) host “update” requests responded during the reporting period
30	srs-cont-check	number of SRS (EPP and any other interface) contact “check” requests responded during the reporting period
31	srs-cont-create	number of SRS (EPP and any other interface) contact “create” requests responded during the reporting period
32	srs-cont-delete	number of SRS (EPP and any other interface) contact “delete” requests responded during the reporting period
33	srs-cont-info	number of SRS (EPP and any other interface) contact “info” requests responded during the reporting period
34	srs-cont-transfer-approve	number of SRS (EPP and any other interface) contact “transfer” requests to approve transfers responded during the reporting period
35	srs-cont-transfer-cancel	number of SRS (EPP and any other interface) contact “transfer” requests to cancel transfers responded during the reporting period
36	srs-cont-transfer-query	number of SRS (EPP and any other interface) contact “transfer” requests to query about a transfer responded during the reporting period
37	srs-cont-transfer-reject	number of SRS (EPP and any other interface) contact “transfer” requests to reject transfers responded during the reporting period
38	srs-cont-transfer-request	number of SRS (EPP and any other interface) contact “transfer” requests to request transfers responded during the reporting period
39	srs-cont-update	number of SRS (EPP and any other interface) contact “update” requests responded during the reporting period

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. No other lines besides the ones described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

For gTLDs that are part of a single-instance Shared Registry System, the Registry Functions Activity Report may include the total contact or host transactions for all the gTLDs in the system.

SPECIFICATION 4

REGISTRATION DATA PUBLICATION SERVICES

1. **Registration Data Directory Services**. Until ICANN requires a different protocol, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <whois.nic.TLD> 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, and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.

   Registry Operator shall implement a new standard supporting access to domain name registration data (SAC 051) no later than one hundred thirty-five (135) days after it is requested by ICANN if: 1) the IETF produces a standard (i.e., it is published, at least, as a Proposed Standard RFC as specified in RFC 2026); and 2) its implementation is commercially reasonable in the context of the overall operation of the registry.

   1.1. The format of responses shall follow a semi-free text format outline below, followed by a blank line and a legal disclaimer specifying the rights of Registry Operator, and of the user querying the database.

   1.2. Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.

   1.3. For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

   1.4. The fields specified below set forth the minimum output requirements. Registry Operator may output data fields in addition to those specified below, subject to approval by ICANN, which approval shall not be unreasonably withheld.

   1.5. **Domain Name Data:**

   1.5.1 **Query format:** whois EXAMPLE.TLD

   1.5.2 **Response format:**

```
Domain Name: EXAMPLE.TLD
Domain ID: D1234567-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
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD
Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 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 Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<
```

1.6. **Registrar Data:**

1.6.1 **Query format**: whois “registrar Example Registrar, Inc.”

1.6.2 **Response format**:

```
Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.tld
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
Admin Contact: Joe Registrar
Phone Number: +1.3105551213
Fax Number: +1.3105551213
Email: joeregistrar@example-registrar.tld
Admin Contact: Jane Registrar
Phone Number: +1.3105551214
Fax Number: +1.3105551213
Email: janeregistrar@example-registrar.tld
Technical Contact: John Geek
Phone Number: +1.3105551215
Fax Number: +1.3105551216
Email: johngeek@example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<
```

1.7. **Nameserver Data:**

1.7.1 **Query format**: whois “NS1.EXAMPLE.TLD”, whois “nameserver (nameserver name)”, or whois “nameserver (IP Address)”

1.7.2 **Response format:**

```
Server Name: NS1.EXAMPLE.TLD
IP Address: 192.0.2.123 IP
Address: 2001:0DB8::1
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 <<<
```

1.8. The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers (the extension will be provided as a separate field as shown above), email addresses, date and times should conform to the mappings specified in EPP RFCs 5730-5734 so that the display of this information (or values return in WHOIS responses) can be uniformly processed and understood.

1.9. In order to be compatible with ICANN's common interface for WHOIS (InterNIC), WHOIS output shall be in the format outline above.

1.10. **Searchability**. Offering searchability capabilities on the Directory Services is optional but if offered by the Registry Operator it shall comply with the specification described in this section.

1.10.1 Registry Operator will offer searchability on the web-based Directory Service.

1.10.2 Registry Operator will offer partial match capabilities, at least, on the following fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.).

1.10.3 Registry Operator will offer exact-match capabilities, at least, on the following fields: registrar id, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records).

1.10.4 Registry Operator will offer Boolean search capabilities supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT.

1.10.5 Search results will include domain names matching the search criteria.

1.10.6 Registry Operator will: 1) implement appropriate measures to avoid abuse of this feature (e.g., permitting access only to legitimate authorized users); and 2) ensure the feature is in compliance with any applicable privacy laws or policies.

1.11. Registry Operator shall provide a link on the primary website for the TLD (i.e., the website provided to ICANN for publishing on the ICANN website) to a web page designated by ICANN containing WHOIS policy and educational materials.

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, which will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider, which may be ICANN or an ICANN designee (the "CZDA Provider"). Registry Operator (optionally through the CZDA Provider) will provide access to zone file data per Section 2.1.3 of this Specification and do so using the file format described in Section 2.1.4 of this Specification. Notwithstanding the foregoing, (a) the CZDA Provider may reject the request for access of any user that does not satisfy the credentialing requirements in Section 2.1.2 below; (b) Registry Operator may reject the request for access of any user that does not provide correct or legitimate credentials under Section 2.1.2 below or where Registry Operator reasonably believes will violate the terms of Section 2.1.5. below; and, (c) Registry Operator may revoke access of any user if Registry Operator has evidence to support that the user has violated the terms of Section 2.1.5 below.

2.1.2 **Credentialing Requirements**. Registry Operator, through the facilitation of the CZDA Provider, will request each user to provide it with information sufficient to correctly identify and locate the user. Such user information will include, without limitation, company name, contact name, address, telephone number, facsimile number, email address and IP address.

2.1.3 **Grant of Access.** Each Registry Operator (optionally through the CZDA Provider) will provide the Zone File FTP (or other Registry supported) service for an ICANN-specified and managed URL (specifically, <TLD>.zda.icann.org where <TLD> is the TLD for which the registry is responsible) for the user to access the Registry's zone data archives. Registry Operator will grant the user a non-exclusive, nontransferable, limited right to access Registry Operator's (optionally CZDA Provider's) Zone File hosting server, and to transfer a copy of the top-level domain zone files, and any associated cryptographic checksum files no more than once per 24 hour period using FTP, or other data transport and access protocols that may be prescribed by ICANN. For every zone file access server, the zone files are in the top-level directory called <zone>.zone.gz, with <zone>.zone.gz.md5 and <zone>.zone.gz.sig to verify downloads. If the Registry Operator (or the CZDA Provider) also provides historical data, it will use the naming pattern <zone>-yyyymmdd.zone.gz, etc.

2.1.4 **File Format Standard**. Registry Operator (optionally through the CZDA Provider) will provide zone files using a subformat of the standard Master File format as originally defined in RFC 1035, Section 5, including all the records present in the actual zone used in the public DNS. Sub-format is as follows:

1. Each record must include all fields in one line as: <domain-name> <TTL> <class> <type> <RDATA>.

2. Class and Type must use the standard mnemonics and must be in lower case.

3. TTL must be present as a decimal integer.

4. Use of /X and /DDD inside domain names is allowed.

5. All domain names must be in lower case.

6. Must use exactly one tab as separator of fields inside a record.

7. All domain names must be fully qualified.

8. No $ORIGIN directives.

9. No use of "@" to denote current origin.

10. No use of "blank domain names" at the beginning of a record to continue the use of the domain name in the previous record.

11. No $INCLUDE directives.

12. No $TTL directives.

13. No use of parentheses, e.g., to continue the list of fields in a record across a line boundary.

14. No use of comments.

15. No blank lines.

16. The SOA record should be present at the top and (duplicated at) the end of the zone file.

17. With the exception of the SOA record, all the records in a file must be in alphabetical order.

18. One zone per file. If a TLD divides its DNS data into multiple zones, each goes into a separate file named as above, with all the files combined using tar into a file called <tld>.zone.tar.

2.1.5 **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 Registry Operator be required or permitted to allow user to use the data to, (i) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar.

2.1.6 **Term of Use**. Registry Operator, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months. Registry Operator will allow users to renew their Grant of Access.

2.1.7 **No Fee for Access**. Registry Operator will provide, and CZDA Provider will facilitate, access to the zone file to user at no cost.

2.2. **Co-operation**

2.2.1 **Assistance**. Registry Operator will co-operate and provide reasonable assistance to ICANN and the CZDA Provider to facilitate and maintain the efficient access of zone file data by permitted users as contemplated under this Schedule.

2.3. **ICANN Access**. Registry Operator shall provide bulk access to the zone files for the TLD to ICANN or its designee on a continuous basis in the manner ICANN may reasonably specify from time to time. Access will be provided at least daily. Zone files will include SRS data committed as close as possible to 00:00:00 UTC.

2.4. **Emergency Operator Access**. Registry Operator shall provide bulk access to the zone files for the TLD to the Emergency Operators designated by ICANN on a continuous basis in the manner ICANN may reasonably specify from time to time.

3. **Bulk Registration Data Access to ICANN**

3.1. **Periodic Access to Thin Registration Data**. In order to verify and ensure the operational stability of Registry Services as well as to facilitate compliance checks on accredited registrars, Registry Operator will provide ICANN on a weekly basis (the day to be designated by ICANN) with up-to-date Registration Data as specified below. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.

3.1.1 **Contents**. Registry Operator will provide, at least, the following data for all registered domain names: domain name, domain name repository object id (roid), registrar id (IANA ID), statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, at least, it will provide: registrar name, registrar repository object id (roid), hostname of registrar Whois server, and URL of registrar.

3.1.2 **Format**. The data will be provided in the format specified in Specification 2 for Data Escrow (including encryption, signing, etc.) but including only the fields mentioned in the previous section, i.e., the file will only contain Domain and Registrar objects with the fields mentioned above. Registry Operator has the option to provide a full deposit file instead as specified in Specification 2.

3.1.3 **Access**. Registry Operator will have the file(s) ready for download as of 00:00:00 UTC on the day designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, though ICANN may request other means in the future.

3.2. **Exceptional Access to Thick Registration Data**. In case of a registrar failure, deaccreditation, court order, etc. that prompts the temporary or definitive transfer of its domain names to another registrar, at the request of ICANN, Registry Operator will provide ICANN with up-to-date data for the domain names of the losing registrar. The data will be provided in the format specified in Specification 2 for Data Escrow. The file will only contain data related to the domain names of the losing registrar. Registry Operator will provide the data as soon as commercially practicable, but in no event later than five (5) calendar days following ICANN's request. Unless otherwise agreed by Registry Operator and ICANN, the file will be made available for download by ICANN in the same manner as the data specified in Section 3.1 of this Specification.

SPECIFICATION 5

SCHEDULE OF RESERVED NAMES

Except to the extent that ICANN otherwise expressly authorizes in writing, and subject to the terms and conditions of this Specification, Registry Operator shall reserve the following labels from initial (i.e., other than renewal) registration within the TLD. If using self-allocation, the Registry Operator must show the registration in the RDDS. In the case of IDN names (as indicated below), IDN variants will be identified according to the registry operator IDN registration policy, where applicable.

1. **Example.** The ASCII label "EXAMPLE" shall be withheld from registration or allocated to Registry Operator at the second level and at all other levels within the TLD at which Registry Operator offers registrations (such second level and all other levels are collectively referred to herein as, "All Levels"). Such label may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, such withheld or allocated label shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such name without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

2. **Two-character labels**. All two-character ASCII labels shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Such labels may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator, provided that such two-character label strings may be released to the extent that Registry Operator reaches agreement with the related government and country-code manager of the string as specified in the ISO 3166-1 alpha-2 standard. The Registry Operator may also propose the release of these reservations based on its implementation of measures to avoid confusion with the corresponding country codes, subject to approval by ICANN. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such labels that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

3. **Reservations for Registry Operations**.

   3.1. The following ASCII labels must be withheld from registration or allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: WWW, RDDS and WHOIS. The following ASCII label must be allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: NIC. Registry Operator may activate WWW, RDDS and WHOIS in the DNS, but must activate NIC in the

DNS, as necessary for the operation of the TLD. None of WWW, RDDS, WHOIS or NIC may be released or registered to any person (other than Registry Operator) or third party. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD all such withheld or allocated names shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

3.2. Registry Operator may activate in the DNS at All Levels up to one hundred (100) names (plus their IDN variants, where applicable) necessary for the operation or the promotion of the TLD. Registry Operator must act as the Registered Name Holder of such names as that term is defined in the then-current ICANN Registrar Accreditation Agreement (RAA). These activations will be considered Transactions for purposes of Section 6.1 of the Agreement. Registry Operator must either (i) register such names through an ICANN-accredited registrar; or (ii) self-allocate such names and with respect to those names submit to and be responsible to ICANN for compliance with ICANN Consensus Policies and the obligations set forth in Subsections 3.7.7.1 through 3.7.7.12 of the then-current RAA (or any other replacement clause setting out the terms of the registration agreement between a registrar and a registered name holder). At Registry Operator's discretion and in compliance with all other terms of this Agreement, such names may be released for registration to another person or entity.

3.3. Registry Operator may withhold from registration or allocate to Registry Operator names (including their IDN variants, where applicable) at All Levels in accordance with Section 2.6 of the Agreement. Such names may not be activated in the DNS, but may be released for registration to another person or entity at Registry Operator's discretion. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Upon ICANN's request, Registry Operator shall provide a listing of all names withheld or allocated to Registry Operator pursuant to Section 2.6 of the Agreement. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

4. **Country and Territory Names**. The country and territory names (including their IDN variants, where applicable) contained in the following internationally recognized lists shall be withheld from registration or allocated to Registry Operator at All Levels:

4.1. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European

Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union <http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm>;

4.2. 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

4.3. 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;

provided, that the reservation of specific country and territory names (including their IDN variants according to the registry operator IDN registration policy, where applicable) may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry Operator must not activate such names in the DNS; provided, that Registry Operator may propose the release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

5. **International Olympic Committee; International Red Cross and Red Crescent Movement**. As instructed from time to time by ICANN, the names (including their IDN variants, where applicable) relating to the International Olympic Committee, International Red Cross and Red Crescent Movement listed at http://www.icann.org/en/resources/registries/reserved shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Additional International Olympic Committee, International Red Cross and Red Crescent Movement names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Such names may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

6. **Intergovernmental Organizations**. As instructed from time to time by ICANN, Registry Operator will implement the protections mechanism determined by the

ICANN Board of Directors relating to the protection of identifiers for Intergovernmental Organizations. A list of reserved names for this Section 6 is available at http://www.icann.org/en/resources/registries/reserved. Additional names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Any such protected identifiers for Intergovernmental Organizations may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such protected identifiers shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

SPECIFICATION 6

REGISTRY INTEROPERABILITY AND CONTINUITY SPECIFICATIONS

1. **Standards Compliance**

1.1. **DNS**. Registry Operator shall 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 the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343, and 5966. DNS labels may only include hyphens in the third and fourth position if they represent valid IDNs (as specified above) in their ASCII encoding (e.g., "xn--ndk061n").

1.2. **EPP**. Registry Operator shall 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 the provisioning and management of domain names using the Extensible Provisioning Protocol (EPP) in conformance with RFCs 5910, 5730, 5731, 5732 (if using host objects), 5733 and 5734. If Registry Operator implements Registry Grace Period (RGP), it will comply with RFC 3915 and its successors. If Registry Operator requires the use of functionality outside the base EPP RFCs, Registry Operator must document EPP extensions in Internet-Draft format following the guidelines described in RFC 3735. Registry Operator will provide and update the relevant documentation of all the EPP Objects and Extensions supported to ICANN prior to deployment.

1.3. **DNSSEC**. Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions ("DNSSEC"). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 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 DNSSEC Practice Statements (DPS) describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material. Registry Operator shall publish its DPS following the format described in RFC 6841.

1.4. **IDN**. If the Registry Operator offers Internationalized Domain Names ("IDNs"), it shall comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registry Operator shall comply with 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.

1.5. **IPv6**. 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 and the recommendations and considerations described in RFC 4472. 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. Registry Operator shall offer public IPv6 transport for its Shared Registration System (SRS) to any Registrar, no later than six (6) months after receiving the first request in writing from a gTLD accredited Registrar willing to operate with the SRS over IPv6.

2. Registry Services

2.1. **Registry Services.** "Registry Services" are, for purposes of the 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.

2.2. **Wildcard Prohibition**. For domain names which are either not registered, 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 RFCs 1034 and 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.

3. Registry Continuity

3.1. **High Availability**. 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 where applicable) to ensure continued operation in the case of technical failure (widespread or local), or an extraordinary occurrence or circumstance beyond the control of the Registry Operator.

3.2. **Extraordinary Event**. Registry Operator will use commercially reasonable efforts to restore the critical functions of the registry within twenty-four (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 forty-eight (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.

3.3. **Business Continuity**. Registry Operator shall maintain a business continuity plan, which will provide for the maintenance of Registry Services in the event of an extraordinary event beyond the control of the Registry Operator or business failure of Registry Operator, and may include the designation of a Registry Services continuity provider. If such plan includes the designation of a Registry Services continuity provider, Registry Operator shall provide the name and contact information for such Registry Services continuity provider to ICANN. 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, if one exists. Registry Operator shall conduct Registry Services Continuity testing at least once per year.

4. Abuse Mitigation

4.1. **Abuse Contact**. Registry Operator shall provide to ICANN and publish 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.

4.2. **Malicious Use of Orphan Glue Records**. Registry Operator shall take action to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

5. Supported Initial and Renewal Registration Periods

5.1. **Initial 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. For the avoidance of doubt, initial registrations of registered names may not exceed ten (10) years.

5.2. **Renewal Periods**. Renewal of registered names may be made in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, renewal of registered names may not extend their registration period beyond ten (10) years from the time of the renewal.

SPECIFICATION 7

MINIMUM REQUIREMENTS FOR RIGHTS PROTECTION MECHANISMS

1. **Rights Protection Mechanisms**. Registry Operator shall implement and adhere to the rights protection mechanisms ("RPMs") specified in this Specification. 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 RPMs required by this Specification 7 and any additional RPMs developed and implemented by Registry Operator in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD. Registry Operator shall implement in accordance with requirements set forth therein each of the mandatory RPMs set forth in the Trademark Clearinghouse as of the date hereof, as posted at [*url to be inserted*] (the "Trademark Clearinghouse Requirements"), which may be revised in immaterial respects by ICANN from time to time. Registry Operator shall not mandate that any owner of applicable intellectual property rights use any other trademark information aggregation, notification, or validation service in addition to or instead of the ICANN-designated Trademark Clearinghouse. If there is a conflict between the terms and conditions of this Agreement and the Trademark Clearinghouse Requirements, the terms and conditions of this Agreement shall control.

2. **Dispute Resolution Mechanisms**. Registry Operator will comply with the following dispute resolution mechanisms as they may be revised from time to time:

   a. the Trademark Post-Delegation Dispute Resolution Procedure (PDDRP) and the Registration Restriction Dispute Resolution Procedure (RRDRP) adopted by ICANN (posted at [urls to be inserted when final procedure is adopted]). Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PDDRP or RRDRP panel and to be bound by any such determination; and

   b. the Uniform Rapid Suspension system ("URS") adopted by ICANN (posted at [url to be inserted]), including the implementation of determinations issued by URS examiners.

SPECIFICATION 8

CONTINUED OPERATIONS INSTRUMENT

1. The Continued Operations Instrument shall (a) provide for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6th) anniversary of the Effective Date, and (b) 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 item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof (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 six (6) years from the Effective Date, and to maintain ICANN as a third party beneficiary thereof. If Registry Operator elects to obtain an irrevocable standby letter of credit but the term required above is unobtainable, Registry Operator may obtain a letter of credit with a one-year term and an "evergreen provision," providing for annual extensions, without amendment, for an indefinite number of additional periods until the issuing bank informs ICANN of its final expiration or until ICANN releases the letter of credit as evidenced in writing, if the letter of credit otherwise meets the requirements set forth in item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof; provided, however, that if the issuing bank informs ICANN of the expiration of such letter of credit prior to the sixth (6th) anniversary of the Effective Date, such letter of credit must provide that ICANN is entitled to draw the funds secured by the letter of credit prior to such expiration. The letter of credit must require the issuing bank to give ICANN at least thirty (30) calendar days' notice of any such expiration or non-renewal. If the letter of credit expires or is terminated at any time prior to the sixth (6th) anniversary of the Effective Date, Registry Operator will be required to obtain a replacement Continued Operations Instrument. ICANN may draw the funds under the original letter of credit, if the replacement Continued Operations Instrument is not in place prior to the expiration of the original letter of credit. 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 sixth 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 critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) anniversary of the Effective Date (an "Alternative Instrument"). Any such Alternative 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 critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) 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 Operator 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 original Continuing Operations Instrument, but shall thereafter apply with respect to such Alternative Instrument(s), and such instrument shall thereafter be considered the Continued Operations Instrument for purposes of this Agreement.

SPECIFICATION 9

REGISTRY OPERATOR CODE OF CONDUCT

1. In connection with the operation of the registry for the TLD, Registry Operator will not, and will not allow any parent, subsidiary, Affiliate, subcontractor or other related entity, to the extent such party is engaged in the provision of Registry Services with respect to the TLD (each, a "Registry Related Party"), to:

   a. directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services, unless comparable opportunities to qualify for such preferences or considerations are made available to all registrars on substantially similar terms and subject to substantially similar conditions;

   b. register domain names in its own right, except for names registered through an ICANN accredited registrar; provided, however, that Registry Operator may (a) reserve names from registration pursuant to Section 2.6 of the Agreement and (b) may withhold from registration or allocate to Registry Operator up to one hundred (100) names pursuant to Section 3.2 of Specification 5;

   c. register names in the TLD or sub-domains of the TLD based upon proprietary access to information about searches or resolution requests by consumers for domain names not yet registered (commonly known as, "front-running"); or

   d. allow any Affiliated registrar to disclose Personal Data about registrants to Registry Operator or any Registry Related Party, except as reasonably necessary for the management and operations of the TLD, unless all unrelated third parties (including other registry operators) are given equivalent access to such user data on substantially similar terms and subject to substantially similar conditions.

2. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will, or will cause such Registry Related Party to, ensure that such services are offered through a legal entity separate from Registry Operator, and maintain separate books of accounts with respect to its registrar or registrar-reseller operations.

3. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will conduct internal reviews at least once per calendar year to ensure compliance with this Code of Conduct. Within twenty (20) calendar days following the end of each calendar year, Registry Operator will provide the results of the internal review, along with a certification executed by an executive officer of Registry Operator certifying as to

Registry Operator's compliance with this Code of Conduct, via email to an address to be provided by ICANN. (ICANN may specify in the future the form and contents of such reports or that the reports be delivered by other reasonable means.) Registry Operator agrees that ICANN may publicly post such results and certification; provided, however, ICANN shall not disclose Confidential Information contained in such results except in accordance with Section 7.15 of the Agreement.

4. Nothing set forth herein shall: (i) limit ICANN from conducting investigations of claims of Registry Operator's non-compliance with this Code of Conduct; or (ii) provide grounds for Registry Operator to refuse to cooperate with ICANN investigations of claims of Registry Operator's non-compliance with this Code of Conduct.

5. Nothing set forth herein shall limit the ability of Registry Operator or any Registry Related Party, to enter into arms-length transactions in the ordinary course of business with a registrar or reseller with respect to products and services unrelated in all respects to the TLD.

6. Registry Operator may request an exemption to this Code of Conduct, and such exemption may be granted by ICANN in ICANN's reasonable discretion, if Registry Operator demonstrates to ICANN's reasonable satisfaction that (i) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator for the exclusive use of Registry Operator or its Affiliates, (ii) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (iii) application of this Code of Conduct to the TLD is not necessary to protect the public interest.

SPECIFICATION 10

REGISTRY PERFORMANCE SPECIFICATIONS

1. **Definitions**

1.1. **DNS**. Refers to the Domain Name System as specified in RFCs 1034, 1035, and related RFCs.

1.2. **DNSSEC proper resolution**. There is a valid DNSSEC chain of trust from the root trust anchor to a particular domain name, e.g., a TLD, a domain name registered under a TLD, etc.

1.3. **EPP**. Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.

1.4. **IP address**. Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.

1.5. **Probes.** Network hosts used to perform (DNS, EPP, etc.) tests (see below) that are located at various global locations.

1.6. **RDDS**. Registration Data Directory Services refers to the collective of WHOIS and Web-based WHOIS services as defined in Specification 4 of this Agreement.

1.7. **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 request will be considered unanswered.

1.8. **SLR**. Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2. **Service Level Agreement Matrix**

	Parameter	**SLR (monthly basis)**
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime (≈ 99%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	≤ 500 ms, for at least 95% of the queries
	DNS update time	≤ 60 min, for at least 95% of the probes
RDDS	RDDS availability	≤ 864 min of downtime (≈ 98%)

	RDDS query RTT	≤ 2000 ms, for at least 95% of the queries
	RDDS update time	≤ 60 min, for at least 95% of the probes
EPP	EPP service availability	≤ 864 min of downtime (≈ 98%)
	EPP session-command RTT	≤ 4000 ms, for at least 90% of the commands
	EPP query-command RTT	≤ 2000 ms, for at least 90% of the commands
	EPP transform-command RTT	≤ 4000 ms, for at least 90% of the commands

Registry Operator is encouraged to do maintenance 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 periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

3. <u>DNS</u>

3.1. **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 DNS probes. For the service to be considered available at a particular moment, at least, two of the delegated name servers registered in the DNS must have successful results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" to which the name server resolves. If 51% or more of the DNS testing probes see the service as unavailable during a given time, the DNS service will be considered unavailable.

3.2. **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/unanswered results from "**DNS tests**" to a name server "**IP address**" during a given time, the name server "**IP address**" will be considered unavailable.

3.3. **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 greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.4. **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 greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.5. **DNS resolution RTT**. Refers to either "**UDP DNS resolution RTT**" or "**TCP DNS resolution RTT**".

3.6. **DNS update time**. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, until 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.

3.7. **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 answer to the query must contain the corresponding information from the Registry System, otherwise 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.

3.8. **Measuring DNS parameters**. Every minute, every DNS probe will make an UDP or TCP "**DNS test**" to each of the public-DNS registered "**IP addresses**" of the name servers of the domain name being monitored. If a "**DNS test**" result is undefined/unanswered, the tested IP will be considered unavailable from that probe until it is time to make a new test.

3.9. **Collating the results from DNS probes**. 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.

3.10. **Distribution of UDP and TCP queries**. DNS probes will send UDP or TCP "**DNS test**" approximating the distribution of these queries.

3.11. **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.

4. <u>RDDS</u>

4.1. **RDDS availability**. Refers to the ability of all the RDDS services for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable.

4.2. **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.

4.3. **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.

4.4. **RDDS query RTT**. Refers to the collective of "**WHOIS query RTT**" and "**Web-based- WHOIS query RTT**".

4.5. **RDDS update time**. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.

4.6. **RDDS test**. Means one query sent to a particular "**IP address**" of one of the servers of one of the RDDS 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 RDDS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.

4.7. **Measuring RDDS parameters**. Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered "**IP addresses**" of the servers for each RDDS service of the TLD being monitored and make an "**RDDS test**" to each one. If an "**RDDS test**" result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.

4.8. **Collating the results from RDDS probes**. 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.

4.9. **Placement of RDDS probes**. Probes for measuring RDDS 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.

5. EPP

5.1. **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. 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.

5.2. **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 2.9.1 of EPP RFC 5730. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.

5.3. **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 or close of either the EPP or 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.

5.4. **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 or close of either the EPP or 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.

5.5. **EPP command RTT**. Refers to "**EPP session-command RTT**", "**EPP query-command RTT**" or "**EPP transform-command RTT**".

5.6. **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.

5.7. **Measuring EPP parameters**. Every 5 minutes, EPP probes will select one "**IP address**" of the EPP servers of the TLD being monitored and make an

"**EPP test**"; every time they should alternate between the 3 different types of commands and between the commands inside each category. If an "**EPP test**" result is undefined/unanswered, the EPP service will be considered as unavailable from that probe until it is time to make a new test.

5.8. **Collating the results from EPP probes**. The minimum number of active testing probes to consider a measurement valid is 5 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.

5.9. **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.

6. Emergency Thresholds

The following matrix presents the emergency thresholds that, if reached by any of the services mentioned above for a TLD, would cause the emergency transition of the Registry for the TLD as specified in Section 2.13 of this Agreement.

Critical Function	Emergency Threshold
DNS Service (all servers)	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP	24-hour total downtime / week
RDDS (WHOIS/Web-based WHOIS)	24-hour total downtime / week
Data Escrow	Breach of the Registry Agreement as described in Specification 2, Part B, Section 6.

7. Emergency Escalation

Escalation is strictly for purposes of notifying and investigating possible or potential issues in relation to monitored services. The initiation of any escalation and the subsequent cooperative investigations do not in themselves imply that a monitored service has failed its performance requirements.

Escalations shall be carried out between ICANN and Registry Operators, Registrars and Registry Operator, and Registrars and ICANN. Registry Operators and ICANN must provide said emergency operations departments. Current contacts must be maintained between ICANN and Registry Operators and published to Registrars, where relevant to their role in escalations, prior to any processing of an Emergency Escalation by all related parties, and kept current at all times.

7.1. Emergency Escalation initiated by ICANN

Upon reaching 10% of the Emergency thresholds as described in Section 6 of this Specification, ICANN's emergency operations will initiate an Emergency Escalation with the relevant Registry Operator. An Emergency Escalation consists of the following minimum elements: electronic (i.e., email or SMS) and/or voice contact notification to the Registry Operator's emergency operations department with detailed information concerning the issue being escalated, including evidence of monitoring failures, cooperative trouble-shooting of the monitoring failure between ICANN staff and the Registry Operator, and the commitment to begin the process of rectifying issues with either the monitoring service or the service being monitoring.

7.2. Emergency Escalation initiated by Registrars

Registry Operator will maintain an emergency operations department prepared to handle emergency requests from registrars. In the event that a registrar is unable to conduct EPP transactions with the registry for the TLD because of a fault with the Registry Service and is unable to either contact (through ICANN mandated methods of communication) the Registry Operator, or the Registry Operator is unable or unwilling to address the fault, the registrar may initiate an emergency escalation to the emergency operations department of ICANN. ICANN then may initiate an emergency escalation with the Registry Operator as explained above.

7.3. Notifications of Outages and Maintenance

In the event that a Registry Operator plans maintenance, it will provide notice to the ICANN emergency operations department, at least, twenty-four (24) hours ahead of that maintenance. ICANN's emergency operations department will note planned maintenance times, and suspend Emergency Escalation services for the monitored services during the expected maintenance outage period.

If Registry Operator declares an outage, as per its contractual obligations with ICANN, on services under a service level agreement and performance requirements, it will notify the ICANN emergency operations department. During that declared outage, ICANN's emergency operations department will note and suspend emergency escalation services for the monitored services involved.

8. <u>Covenants of Performance Measurement</u>

8.1. **No interference**. Registry Operator shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registry Operator shall respond to the measurement tests described in this Specification as it would to any other request from an Internet user (for DNS and RDDS) or registrar (for EPP).

8.2. **ICANN testing registrar**. Registry Operator agrees that ICANN will have a testing registrar used for purposes of measuring the **SLR**s described above. Registry Operator agrees to not provide any differentiated treatment for the testing registrar other than no billing of the transactions. ICANN shall not use the registrar for registering domain names (or other registry objects) for itself or others, except for the purposes of verifying contractual compliance with the conditions described in this Agreement.

SPECIFICATION 11

PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on 27 June 2013 in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. (Intentionally omitted. Registry Operator has not included commitments, statements of intent or business plans provided for in its application to ICANN for the TLD.)

3. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

    a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

    b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

    c. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies.

    d. Registry Operator of a "Generic String" TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person's or entity's "Affiliates" (as defined in Section 2.9(c) of the Registry Agreement). "Generic String" means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others.

4. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

   The above Section 4 of this Specification applies to the following public interest commitments of Registry Operator related to the TLD. Nothing in Section 4 of this Specification shall limit any obligations of Registry Operator under Sections 1, 2 and 3 of this Specification. In the event Section 4 of this Specification conflicts with the requirements of any other provision of the Registry Agreement (including any Section of this Specification), such other provision shall govern.

   a. **Open registration** - Second level registrations in the TLD will be open and available to lawful registrants. The TLD represents a generic or dictionary term, and Registry Operator accordingly will operate it in an inclusive manner. Registry Operator will not limit registrant eligibility based on identity nor restrict availability of second level names to only registrants whose identity is associated only with the most common usage of the term. Registry Operator will not disenfranchise lawful users who are associated with a minority usage of the term.

   b. **Geographic name protection** - Pursuant to Specification 5 of this Registry Agreement, Registry Operator will transmit to registrars the list of geographic names prohibited from second level registration. Registry Operator will periodically review this list to ensure it is identical to that maintained by ICANN. Should Registry Operator seek to release these reserved names, it will consult with ICANN's Governmental Advisory Committee and obtain any permissions necessary from ICANN for such release.

   c. **Rights Protection Mechanisms and Abuse Mitigation** - Registry Operator commits to implementing and performing the following protections for the TLD:

      i. In order to help registrars and registrants identify inaccurate data in the Whois database, Registry Operator will audit Whois data for accuracy on a statistically significant basis (this commitment will be considered satisfied by virtue of and for so long as ICANN conducts such audits).

ii. Work with registrars and registrants to remediate inaccurate Whois data to help ensure a more accurate Whois database. Registry Operator reserves the right to cancel a domain name registration on the basis of inaccurate data, if necessary.

iii. Establish and maintain a Domains Protected Marks List (DPML), a trademark protection service that allows rights holders to reserve registration of exact match trademark terms and terms that contain their trademarks across all gTLDs administered by Registry Operator under certain terms and conditions.

iv. At no cost to trademark holders, establish and maintain a Claims Plus service, which is a notice protection mechanism that begins at the end of ICANN's mandated Trademark Claims period.

v. Bind registrants to terms of use that define and prohibit illegal or abusive activity.

vi. Limit the use of proxy and privacy registration services in cases of malfeasance.

vii. Consistent with the terms of this Registry Agreement, reserve the right to exclude from distribution any registrars with a history of non-compliance with the terms of the Registrar Accreditation Agreement.

viii. Registry Operator will be properly resourced to perform these protections.

d. **Anti-Abuse Policy**

i. Registry Operator's Anti-Abuse Policy will be required under the Registry Registrar Agreement and posted on the Registry Operator's web site.

ii. Registry Operator will monitor the TLD for abusive behavior and address it as soon as possible if detected.

iii. Registry Operator reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any of the following reasons:

A. to protect the integrity and stability of the registry;

B. to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;

C. to comply with the terms of this Registry Agreement and the Registry Operator's Anti-Abuse Policy;

D. registrant fails to keep Whois information accurate and up-to-date;

E. domain name use violates the Registry Operator's acceptable use policies, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark; or

F. as needed during resolution of a dispute.

iv. Abuse Point of Contact. Registry Operator will provide an abuse point of contact (APOC). This contact will be a role-based e-mail address posted on the Registry Operator's web site in the form such as abuse123@registry.tld. This e-mail address will allow multiple staff members to monitor and address abuse reports. Registry Operator will further provide a convenient web form for complaints.

The public interest commitments set forth in this Section 4 of this Specification shall be subject to review by Registry Operator starting in January 2016, and Registry Operator, in its sole discretion and upon written notice to ICANN, may elect at that time to discontinue any of such public interest commitments in the case of a substantial and compelling business need.

Attachment 5

[Corn Lake Request for Addl Submission re GAC Advice]

RE: EXP/395/ICANN/12 (c. EXP/399/ICANN/16, EXP/400/ICANN/17) (.CHARITY)

Don Moody <don@newgtlddisputes.com>

Tue 12/3/2013 7:45 PM

To Contact Information Redacted

Cc Contact Information Redacted

2 attachments

Annex A.pdf; Annex B.pdf;

Dear ICC, Expert Panel, Parties and Counsel:

Applicant respectfully submits the following information to update the Panel regarding matters raised in the Objection and further submissions made by the Objector.

Among other things, Objector has argued that the Application creates a likelihood of material detriment to the alleged community due to an alleged lack of the types of safeguards proposed by the GAC in its Beijing Communiqué of April 2013. Please be advised that, per the attached Annex A -- copy also available at: https://www.icann.org/en/news/correspondence/crocker-to-dryden-3-29oct13-en.pdf -- ICANN has formally announced its intention to adopt the "GAC's Beijing Communiqué advice concerning Category 1 and Category 2 Safeguards," which the GAC responded to in a follow-up communiqué issued during the recently-conducted meetings in Buenos Aires. See Annex B and http://www.icann.org/en/news/correspondence/gac-to-board-20nov13-en.pdf.

To the extent ICANN has so adopted the GAC advice, Applicant must implement the safeguards, if awarded the subject string, as a term of its registry agreement with ICANN for the string. Applicant therefore respectfully submits that, to the extent Objector claims material detriment based on Applicant's alleged lack of GAC-recommended safeguards, ICANN's recent action has rendered that portion of the Objection moot, and eliminates it as a basis for denying Applicant its presumptive right to compete for and, if awarded, operate the string.

Sincerely,

Don C. Moody, J.D., M.S.
New gTLD Disputes
Registered USPTO
Contact Information Redacted

Contact Information Redacted

Tel: Contact nformation Redacted | Cell: Contact nformation Redacted
eFax: Contact nformation Redacted | eMail: Contact Information Redacted

ANNEX A

[Letter from Stephen D. Crocker, Chair, ICANN Board of Directors to Heather Dryden, Chair, Governmental Advisory Committee, dated October 29, 2013]

29 October 2013

Heather Dryden
Chair, Governmental Advisory Committee

Re: NGPC Consideration of GAC Category 1 and Category 2 Safeguard Advice

Dear Heather,

On behalf of the New gTLD Program Committee, I am pleased to inform you that the NGPC is intending to accept the GAC's Beijing Communiqué advice concerning Category 1 and Category 2 Safeguards. Attached please find documents that describe how ICANN intends to implement the advice. A summary of the implementation plans appears below.

Category 1 Safeguards

The text of the Category 1 Safeguards have been modified as appropriate to meet the spirit and intent of the advice in a manner that allows the requirements to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement ("PIC Spec"). The PIC Spec and a rationale explaining the modifications are attached.

The implementation plan also distinguishes the list of TLD strings listed in the Category 1 safeguard advice between strings that the NGPC considers strings associated with market sectors or industries that have highly regulated entry requirements in multiple jurisdictions, and those that do not. The Category 1 Safeguards in the PIC Spec will apply to the TLD strings based on how the TLD string is categorized. The list of re-categorized Category 1 strings is attached.

Category 2 Safeguards

ICANN contacted the 186 applicants for strings identified in the GAC's Category 2 safeguard advice. The applicants were asked to respond by a specified date indicating whether the applied-for TLD will be operated as an exclusive access registry. An overwhelming majority of the applicants (174) indicated that the TLD would not be operated as an exclusive access registry. The NGPC recently adopted a resolution directing staff to move forward with the contracting process for applicants for strings identified in the Category 2 Safeguards that were prepared to enter into the Registry Agreement as approved, since moving forward with these applicants was consistent with the GAC's advice.

Ten applicants responded that the TLD would be operated as an exclusive access registry. These 10 applicants have applied for the following strings: .BROKER, .CRUISE, .DATA, .DVR, .GROCERY, .MOBILE, .PHONE, .STORE, .THEATER, .THEATRE and .TIRES. The NGPC directed staff to prepare an analysis and proposal to implement the Category 2 safeguard advice for these applicants. Staff requested the applicants to provide an explanation of how the proposed exclusive registry access serves a public interest goal. When available, the responses will be forwarded to the NGPC and the GAC for further consideration.

I hope this information is helpful. I look forward to seeing you at the ICANN 48 Meeting in Buenos Aires.

Best regards,

Stephen D. Crocker
Chair, ICANN Board of Directors

Category 1 Safeguards as Public Interest Commitments in Specification 11 of the New gTLD Registry Agreement

1. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring registrants to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

2. Registry operators will include a provision in their Registry-Registrar Agreements that requires registrars at the time of registration to notify registrants of the requirement to comply with all applicable laws.

3. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

4. Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self-regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication, including for the purpose of facilitating the development of a strategy to mitigate the risks of fraudulent and other illegal activities.

5. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to provide administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

6. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.

7. If a Registry Operator receives a complaint expressing doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents regarding the authenticity.

8. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision

requiring Registrants to report any material changes to the validity of the Registrants' authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

9. Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.

GAC Category 1 Safeguard Advice
Rationale for Changes to Safeguard Language in the PIC Spec

The NGPC intends to adapt the language of the Category 1 safeguards to meet the spirit and intent of the GAC's Category 1 Safeguard Advice in a manner that allows the safeguards to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement (the "Category 1 PIC Spec").

Safeguards #1, #2 and #5

Because registry operators and ICANN do not have contractual relationships with registrants, additional language was added to Safeguards #1, #2 and #5 to refer to Registry-Registrar Agreements and Registration Agreements to impose the obligation on registrants required in the safeguard advice.

Safeguard #3

Safeguard #3 would require registrants to implement reasonable and appropriate security measures if the registrant collects and maintains sensitive health and financial data. The security measures should be commensurate with the offering of those services, as defined by applicable law and recognized industry standards. The NGPC notes that implementation would not be possible because it is not clear how "recognized industry standards" would be identified and applied in the context of hundreds of different sectors.

The language in the PIC Spec to address this safeguard was adapted to require that the security measures are commensurate with the offering of those services, as defined by applicable law.

Safeguard #4

The NGPC notes that the safeguard raises contract enforcement questions (e.g., how are the relevant regulatory agencies and industry self-regulatory organizations identified; who determines which industry self-regulation organizations bodies are "relevant" to a particular string and which governmental body is the competent regulatory agency). Additionally, some regulatory bodies or industry self-regulatory bodies may not be responsive to collaboration with registry operators.

To address these concerns, the safeguard language in the PIC Spec was drafted in a way to avoid a situation where the registry operator would be in breach of the registry agreement if regulatory body won't agree to a relationship with the registry operator.

Safeguards #6, #7 and #8

The implementation of safeguards #6-8 would change the nature of some new gTLDs from being open to uses that are not regulated into restricted TLDs open only to registrants that can prove their status or credentials. The NGPC also notes that implementation would potentially discriminate against users in developing nations whose governments do not have regulatory bodies or keep databases which a registry/registrar could work with to verify credentials, and would potentially discriminate against users in developed nations whose governments have developed different regulatory regimes.

The language in the Category 1 PIC Spec was modified to address these concerns. As an initial matter, the registrant would be required to make an attestation that the registrant possesses any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD string. The registrant is also required to report any material changes to the validity of their authorizations. This provision provides the registrant the opportunity to provide this information because it is better positioned to

If the registry operator receives complaints about the authenticity of the licenses or credentials, the registry operator is obligated to consult with the relevant national supervisory authorities, or their equivalents regarding the authenticity.

GAC Category 1 Strings

Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-3 applicable)	**Highly-regulated Sectors/Closed Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-8 applicable)**
Children: .kid, .kids, .kinder, .game, .games, .juegos, .play, .school, .schule, toys	
Environmental: .earth, .eco, .green, .bio, .organic	
Health and Fitness: .care, .diet, .fit, .fitness, .health, .heart, .hiv, .rehab, .clinic, .healthy (IDN Chinese equivalent), .dental, .physio, .healthcare, .med, .organic, .doctor	**Health and Fitness:** pharmacy, .surgery, .dentist , .dds, , .hospital, .medical
Financial: capital, . cash, .cashbackbonus, .broker, .brokers, .claims, .exchange, .finance, .financial, .forex, .fund, .investments, .lease, .loan, .loans, .market, . markets, .money, .pay, .payu, .retirement, .save, .trading, .credit, .insure, .netbank, .tax, .travelersinsurance, .financialaid, .vermogensberatung, .mortgage, .reit	**Financial:** .bank, .banque, .creditunion, .creditcard, .insurance, .ira, .lifeinsurance, .mutualfunds, .mutuelle, .vermogensberater, and .vesicherung, .autoinsurance, .carinsurance
	Gambling: .bet, .bingo, .lotto, .poker,.spreadbetting, .casino
Charity: .care, .gives, .giving	**Charity:** .charity (and IDN Chinese equivalent)
Education: .degree, .mba	**Education:** .university
Intellectual Property: .audio, .book (and IDN equivalent), .broadway, .film, .game, .games, .juegos, .movie, .music, .software, .song, .tunes,	

Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions **(Category 1 Safeguards 1-3 applicable)**	**Highly-regulated Sectors/Closed Entry Requirements in Multiple Jurisdictions** **(Category 1 Safeguards 1-8 applicable)**
.fashion (and IDN equivalent), .video, .app, .art, .author, .band, .beats, .cloud (and IDN equivalent), .data, .design, .digital, .download, .entertainment, .fan, .fans, .free, .gratis, .discount, .sale, .hiphop, .media, .news, .online, .pictures, .radio, .rip, .show, .theater, .theatre, .tour, .tours, .tvs, .video, .zip	
Professional Services: .accountant, .accountants, .architect, .associates, .broker, .brokers, .engineer, .legal, .realtor, .realty, .vet, .doctor, .engineering, .law	**Professional Services:** .abogado, .attorney, .cpa, .dentist, .dds, .lawyer.
Corporate Identifiers: .limited	**Corporate Identifiers:** .corp, .gmbh, .inc, .llc, .llp, .ltda, .ltd, .sarl, .srl, .sal
Generic Geographic Terms: .capital .town, .city	
.reise, .reisen .weather	

Special Safeguards Required

Inherently Governmental Functions: .army, .navy, .airforce
Potential for Cyber Bullying/Harassment: .fail, .gripe, .sucks, .wtf

Category 1 Safeguards as Public Interest Commitments in Specification 11 of the New gTLD Registry Agreement

1. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring registrants to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

2. Registry operators will include a provision in their Registry-Registrar Agreements that requires registrars at the time of registration to notify registrants of the requirement to comply with all applicable laws.

3. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

4. Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self-regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication, including for the purpose of facilitating the development of a strategy to mitigate the risks of fraudulent and other illegal activities.

5. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to provide administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

6. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.

7. If a Registry Operator receives a complaint expressing doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents regarding the authenticity.

8. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to report any material changes to the validity of the Registrants' authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

9. Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.

ANNEX B

[GAC Buenos Aires Communiqué, dated November 20, 2013]

Governmental Advisory Committee

Buenos Aires, 20 November 2013

GAC Communiqué – Buenos Aires, Argentina

I. Introduction

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Buenos Aires during the week of 16 November 2013. 56 GAC Members attended the meetings, with one GAC Member participating remotely, and five Observers. The GAC expresses warm thanks to the local host, NIC Argentina, for their support.

At the beginning of its meeting the GAC expressed its sympathy for and solidarity with the people and government of the Philippines following the recent disaster of Typhoon Haiyan.

II. GAC Advice to the Board[1]

1. Category 1 and Category 2 Safeguard Advice

The GAC welcomed the response of the Board to the GAC's Beijing Communiqué advice on Category 1 and Category 2 safeguards. The GAC received useful information regarding implementation of the safeguards during its discussions with the New gTLD Program Committee. GAC members asked for clarification of a number of issues and look forward to ICANN's response.

a. The GAC highlights the importance of its Beijing advice on 'Restricted Access' registries, particularly with regard to the need to avoid undue preference and/or undue disadvantage.

   i. **The GAC requests**

      1. A briefing on whether the Board considers that the existing PIC specifications (including 3c) fully implements this advice.

b. The GAC requests a briefing on the public policy implications of holding auctions to resolve string contention (including community applications).

[1] To track the history and progress of GAC Advice to the Board, please visit the GAC Advice Online Register available at: https://gacweb.icann.org/display/GACADV/GAC+Register+of+Advice

c. The GAC considers that new gTLD registry operators should be made aware of the importance of protecting children and their rights consistent with the UN Convention on the Rights of the Child.

d. **The GAC advises the ICANN Board:**

   i. to re-categorize the string .doctor as falling within Category 1 safeguard advice addressing highly regulated sectors, therefore ascribing these domains exclusively to legitimate medical practitioners. The GAC notes the strong implications for consumer protection and consumer trust, and the need for proper medical ethical standards, demanded by the medical field online to be fully respected.

e. The GAC welcomes the Board's communication with applicants with regard to open and closed gTLDs, but seeks **written clarification** of how strings are identified as being generic.

2. **GAC Objections to Specific Applications (ref. Beijing Communiqué 1.c.)**

   a. .guangzhou (IDN in Chinese), .shenzhen (IDN in Chinese), and .spa

   Discussions between interested parties are ongoing so as noted in the Durban Communiqué

      i. **The GAC advises the ICANN Board**:

         1. Not to proceed beyond initial evaluation until the agreements between the relevant parties are reached.

            a. The application for .guangzhou (IDN in Chinese – application number 1-1121-22691)

            b. The application for .shenzhen (IDN in Chinese – 1-1121-82863)

            c. The applications for .spa (application number 1-1309-12524 and 1-1619-92115)

   b. The GAC notes that the application for .yun (application number 1-1318-12524) has been withdrawn.

   c. The GAC welcomes the Board's acceptance of its advice in the Durban Communiqué on the application for .thai.

   d. The GAC sought an update from the Board on the current status of the implementation of the GAC Advice for .amazon.

3. **.wine and .vin**

   The GAC took note of the developments on the two strings .wine and .vin from its previous meetings in Beijing and Durban.

   GAC members have undertaken extensive discussions to examine a diversity of views on these applications, and the protections associated with Geographical Indications (GIs).

GAC considers that appropriate safeguards against possible abuse of these new gTLDs are needed.

Some members are of the view, after prolonged and careful consideration, that the existing safeguards outlined in the GAC's Beijing Communiqué and implemented by the ICANN Board are appropriate and sufficient to deal with the potential for misuse of the .wine and .vin new gTLDs. These members welcome the Board's response to these safeguards, which prohibit fraudulent or deceptive use of domain names. They consider that it would be inappropriate and a serious concern if the agreed international settings on GIs were to be redesigned by ICANN. The current protections for geographical indications are the outcome of carefully balanced negotiations. Any changes to those protections are more appropriately negotiated among intellectual property experts in the World Intellectual Property Organization and the World Trade Organization.

Other members consider that delegation of .wine and.vin strings should remain on hold until either sufficient additional safeguards to protect GIs are put into place in these strings to protect the consumers and businesses that rely on such GIs; or common ground has been reached for the worldwide protection of GIs via international fora and wide array of major trade agreements. Given this changing context, they welcome the current face-to-face talks between the applicants for .wine and .vin. and wine producers, aiming to protect their assets and consumers' interests whilst taking into account governments' public policy concerns.

The Board may wish to seek a clear understanding of the legally complex and politically sensitive background on this matter in order to consider the appropriate next steps in the process of delegating the two strings. GAC members may wish to write to the Board to further elaborate their views.

4. Protection of Inter-Governmental Organisations (IGOs)

a. The GAC Advises the ICANN Board that:

i. The GAC, together with IGOs, remains committed to continuing the dialogue with NGPC on finalising the modalities for permanent protection of IGO acronyms at the second level, by putting in place a mechanism which would:

1. provide for a permanent system of notifications to both the potential registrant and the relevant IGO as to a possible conflict if a potential registrant seeks to register a domain name matching the acronym of that IGO;
2. allow the IGO a timely opportunity to effectively prevent potential misuse and confusion;
3. allow for a final and binding determination by an independent third party in order to resolve any disagreement between an IGO and a potential registrant; and
4. be at no cost or of a nominal cost only to the IGO.

The GAC looks forward to receiving the alternative NGPC proposal adequately addressing this advice. The initial protections for IGO acronyms should remain in place until the dialogue between the NGPC, the IGOs and the GAC ensuring the implementation of this protection is completed.

5. **Special Launch Program for Geographic and Community TLDs**

   The GAC recognizes the importance of the priority inclusion of government and locally relevant name strings for the successful launch and continued administration of community and geographic TLDs.

   The GAC appreciates that the Trademark Clearing House (TMCH) is an important rights protection mechanism applicable across all the new gTLDs and has an invaluable role to fulfill across the new gTLD spectrum as a basic safety net for the protection of trademark rights.

   a. **The GAC Advises the ICANN Board:**

      i. that ICANN provide clarity on the proposed launch program for special cases as a matter of urgency.

6. **Protection of Red Cross/Red Crescent Names**

   a. The GAC advises the ICANN Board:

      i. that it is giving further consideration to the way in which existing protections should apply to the words “Red Cross”, “Red Crescent” and related designations at the top and second levels with specific regard to national Red Cross and Red Crescent entities; and that it will provide further advice to the Board on this.

7. **.islam and .halal**

   a. GAC took note of letters sent by the OIC and the ICANN Chairman in relation to the strings .islam and .halal. The GAC has previously provided advice in its Beijing Communiqué, when it concluded its discussions on these strings. The GAC Chair will respond to the OIC correspondence accordingly, noting the OIC’s plans to hold a meeting in early December. The GAC chair will also respond to the ICANN Chair's correspondence in similar terms.

III. Inter-constituencies Activities

1. **Meeting with the Generic Names Supporting Organisation (GNSO)**

   The GAC met with the GNSO and welcomed preliminary work that has been done to identify improved ways for earlier GAC involvement in policy development processes which have potential public policy aspects. A joint GAC/GNSO working group will be established to develop inter-sessionally more detailed options for implementation.

2. **Meeting with the Expert Working Group on gTLD Directory Services (EWG)**

The GAC met with the EWG and exchanged views on the model proposed by the EWG for next generation directory services. GAC members highlighted a range of issues including the importance of applicable data privacy laws, the balance between public and restricted data elements, and the accreditation process to allow access to restricted data for legitimate purposes. The GAC welcomed the opportunity for continuing engagement with the EWG.

3. **Meeting with the Country Code Names Supporting Organisation (ccNSO)**

   The GAC met with the ccNSO and received briefings on ccNSO working groups on the IDN policy development process and the framework of interpretation; and the study group on country names. The GAC committed to continuing engagement with these issues, all of which have public policy implications, and will continue to work closely with the ccNSO.

4. **Meeting with the Accountability and Transparency Review Team 2 (ATRT 2)**

   The GAC is grateful for the work undertaken by the ATRT2 and discussed with review team members their draft recommendations and report, noting that it was valuable to gain an external perspective on the work and operations of the GAC. The GAC has already made progress in relation to early engagement in policy development processes, increased transparency and improved working methods, but acknowledges that there is always more to be done, particularly in outreach. GAC members noted that the GAC provides policy advice, not legal advice. The GAC noted that each member already operates within their own government's code of conduct framework.

5. **Meeting with the Brand Registry Group (BRG)**

   The GAC met with the Brand Registry Group to discuss their proposal for a streamlined process under an addendum to the Registry Agreement for the approval of country names and 2-letter and character codes at the second level. The GAC undertook to consider this proposal further and respond to the BRG in due course.

***

The GAC warmly thanks the GNSO, the EWG, the ccNSO, and the ATRT 2, who jointly met with the GAC; as well as all those among the ICANN community who have contributed to the dialogue with the GAC in Buenos Aires.

IV. Internal Matters

1. **New Members and Observers** - The GAC welcomes the Commonwealth of Dominica and Montenegro as members, and the Organisation of Islamic Cooperation and the Caribbean Telecommunications Union as observers.

2. **GAC Secretariat** – The independent consultants, Australian Continuous Improvement Group, have begun providing additional secretariat services to the

GAC. A range of measures to improve the efficiency and effectiveness of the GAC is being progressively implemented.

3. **GAC Leadership** - The GAC welcomed the re-election of the current Vice Chairs (Australia, Switzerland and Trinidad and Tobago) for a further term. The issue of a possible increase in the number of Vice Chairs to better represent regions and manage workload has been referred to the GAC working group on working methods for consideration and report.

4. **New gTLDs** - At the ICANN meeting in Durban, the GAC formed a working group to begin consideration of potential public policy input for future rounds of new gTLDs. This working group has been focusing on issues associated with the protection of geographic names, the processes associated with identified communities, and developing economy issues and applicant support. The outcomes of the Geographic names working group are expected to be presented to the community by the ICANN 49 Singapore meeting. The GAC looks forward to discussing these issues with the community in future meetings.

5. **Working Methods** – At the ICANN meeting in Durban the GAC formed a working group to consider improvements to the GAC's working methods. A range of immediate measures has been identified and is being progressively implemented. Other matters will be progressed in coordination with related initiatives including the ATRT 2 process.

6. **High Level Meeting** - A high level meeting of governments will be held in London in June 2014 in conjunction with the ICANN and GAC meetings. The agenda for the meeting should be finalised in Singapore.

V. Next Meeting

The GAC will meet during the period of the 49th ICANN meeting in Singapore.

Attachment 6

[IO Response to Corn Lake Request for Addl Submission]

Re: EXP/395/ICANN/12 (c. EXP/399/ICANN/16, EXP/400/ICANN/17) (.CHARITY)

Alain Pellet <contact@independent objector newgtlds.org>

Thu 12/5/2013 1:25 PM

To Contact Information Redacted

Cc Contact Information Redacted

Dear Expert Panel,

I am writing in response to Mr Moody's email received on 4 December 2013.

I note that, pursuant to Article 17 (a) of the attachment to Module 3 of the Applicant Guidebook, New gTLD Dispute Resolution Procedure (hereinafter "the Procedure"), "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". I therefore request the Expert Panel to dismiss this unsolicited additional statement which was not submitted in accordance with the Procedure.

Should the Expert Panel accept this new submission, I wish to prevail myself of the right to respond in accordance with Article 4 of the Procedure, which stipulates that the Expert Panel shall "ensure that the parties are treated with equality, and that each party is given a reasonable opportunity to present its position".

In any case, I wish to emphasize that in its authorized additional written statement, the Applicant submitted that "objector places great weight on the GAC's Beijing communiqué, when in fact it has no relevance to the Objection." Obviously, instead of strengthening the Applicant's previous submission, this new email highlights its lack of incoherence and consistency.

Sincerely,

Alain PELLET
ICANN – Independent Objector

Le 4 déc. 2013 à 04:45, "Don Moody"Contact Information Redacted a écrit :

> Dear ICC, Expert Panel, Parties and Counsel:
>
> Applicant respectfully submits the following information to update the Panel regarding matters raised in the Objection and further submissions made by the Objector.
>
> Among other things, Objector has argued that the Application creates a likelihood of material detriment to the alleged community due to an alleged lack of the types of safeguards proposed by the GAC in its Beijing Communiqu? of April 2013. Please be advised that, per the attached Annex A -- copy also available at: https://www.icann.org/en/news/correspondence/crocker-to-dryden-3-29oct13-en.pdf -- ICANN has formally announced its intention to adopt the "GAC's Beijing Communiqu? advice concerning Category 1 and Category 2 Safeguards," which the GAC responded to in a follow-up communiqu? issued during the recently-conducted meetings in Buenos Aires. See Annex B and http://www.icann.org/en/news/correspondence/gac-to-board-20nov13-en.pdf.

To the extent ICANN has so adopted the GAC advice, Applicant must implement the safeguards, if awarded the subject string, as a term of its registry agreement with ICANN for the string. Applicant therefore respectfully submits that, to the extent Objector claims material detriment based on Applicant's alleged lack of GAC-recommended safeguards, ICANN's recent action has rendered that portion of the

Objection moot, and eliminates it as a basis for denying Applicant its presumptive right to compete for and, if awarded, operate the string.

Sincerely,

Don C. Moody, J.D , M.S.

New gTLD Disputes

Registered USPTO

Contact Information Redacted

<Annex A.pdf>

<Annex B.pdf>

Attachment 7

[Panel Denial of Corn Lake Request for Addl Submission]

RE: EXP/395/ICANN/12 (c. EXP/399/ICANN/16, EXP/400/ICANN/17)

PORTWOOD Tim <timportwood@bredinprat.com>

Fri 12/13/2013 1:57 AM

To Contact Information Redacted

Cc Contact Information Redacted

1 attachment

131212 Letter to Parties.pdf;

Dear Party Representatives,

Please find attached the Expert Panel's letter of today's date.

Yours sincerely,

Tim Portwood
Avocat à la Cour
Barrister of England & Wales
Contact Information Redacted

Bredin Prat est constitué sous forme d'AARPI.

Ce courrier électronique et ses pièces jointes sont couverts par la confidentialité ou le secret professionnel.

This e-mail and any attachments hereto are privileged and confidential.

De : READE Emma Contact Information Redacted **De la part de** EXPERTISE
Envoyé : mercredi 11 décembre 2013 19:15
Contact Information Redacted
Cc : Contact Information Redacted
Objet : EXP/395/ICANN/12 (c. EXP/399/ICANN/16, EXP/400/ICANN/17)

Dear Sirs,

The Centre acknowledges receipt of Mr. Don Moody's e-mail of 4 December 2013, sent on behalf of the Applicant, a copy of which was sent to the Independent Objector and the Expert Panel directly.

The Centre further acknowledges receipt of Mr. Alain Pellet, Independent Objector's e-mail of 5 December 2013, a copy of which was sent to the Applicant and to the Expert Panel directly.

The Centre would like to draw your attention to the fact that ICANN's New gTLD Dispute Resolution Procedure does not provide for any specific provision regarding the issue raised by the Applicant. Accordingly, the Centre has referred the decision of whether to take the Applicant's additional information into account to the Expert Panel.

Should the Expert Panel decide to reopen this matter and accept further submissions by the parties, the Expert Panel will inform you accordingly.

In this regard please also be informed that the draft Expert Determination as submitted by the Expert Panel to the Centre is currently in the scrutiny procedure. Unless the Expert Panel decides to reopen the proceeding and revise the Expert Determination, the Centre shall continue the scrutiny process on the draft Expert Determination as submitted.

Please do not hesitate to contact us if you have any further questions,

Best regards,

Emma Reade | Juriste
International Centre for ADR | International Chamber of Commerce
Contact Information Redacted

BREDIN PRAT

Ms Héloïse Bajer-Pellet
Contact Information Redacted

Mr Daniel Müller
mail@muellerdaniel.eu

Mr Phon van den Biesen
Contact Information Redacted

Mr Sam Wordsworth
Contact Information Redacted

The IP and Technology Legal Group PC
Mr John M. Genga and Don C. Moody
Contact Information Redacted

Ms Pam Little
Contact Information Redacted

Famous Four Media Limited
Mr Peter Young
Contact Information Redacted

Copy :
ICC International Centre for Expertise
Contact Information Redacted

Paris, 13 December 2013

Re: **EXP/395/ICANN/12 (c. EXP/399/ICANN/16 & EXP/400/ICANN/17)**
Prof. Alain Pellet, Independent Objector (France) vs/ Corn Lake, LLC (USA) **and** Prof. Alain Pellet, Independent Objector (France) vs/ Excellent First Limited (Cayman Islands) **and** Prof. Alain Pellet, Independent Objector (France) vs/ Spring Registry Limited (Gibraltar)

Dear Party Representatives,

The Expert is writing to you with respect to Applicant Corn Lake, LLC's email dated 4 December 2013 and the Independent Objector's response dated 5 December 2013.

In its email of 4 December 2013, Applicant Corn Lake LLC made further submissions with respect to the defence of its Application (the "**Further Submissions**").

In its email in response of 5 December 2013, the Independent Objector objected to those further submissions on both procedural and substantive grounds (the "**Objector's Response**").

On 11 December 2013, the International Centre for ADR of the ICC (the "**Centre**") wrote separately to the Parties and to the Expert Panel reserving to the Expert Panel the decision as to whether to admit the Parties' further submissions into the proceeding.

The Further Submissions were not contemplated by the procedural timetable (as amended) set out in the Expert Panel's communication of 9 August 2013 under Article 17(a) of the Procedure.

The Expert Determination in each of the consolidated cases was submitted in draft to the Centre within the 45 day time period provided for in Article 21(a) of the ICANN New gTLD Dispute Resolution Procedure (the "**Procedure**") for scrutiny by the Centre pursuant to Article 21(b) of the Procedure and Article 12(6) of the ICC Rules for Expertise (the "**Rules**"). No application by the Expert Panel had therefore been made to the Centre for an extension of that 45 day time period under Article 21(a) of the Procedure. The Parties were therefore fully aware that the draft Expert Determinations were in the Centre's hands for the scrutiny process at the time the Further Submissions were made.

No application was made by Applicant Corn Lake, LLC to seek leave of the Expert Panel to make the Further Submissions.

In light of the foregoing procedural considerations, the Expert Panel determines to dismiss the Further Submissions and therefore the substantive content of the Objector's Response.

Yours sincerely,

Tim Portwood
Contact Information Redacted

Cc: Prof. Alain Pellet, Independent Objector
Contact Information Redacted

Mr Daniel Schindler, Corn Lake, LLC
cornlake@donuts.co

Mr. Ching Hong Seng, Excellent First Limited
Contact Information Redacted

Mr Geir Andreas Rasmussen, Spring Registry Limited
Contact Information Redacted

Attachment 8

[Ruling]

THE INTERNATIONAL CENTRE FOR EXPERTISE OF THE

INTERNATIONAL CHAMBER OF COMMERCE

CASE No. EXP/395/ICANN/12

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR

(FRANCE)

vs/

CORN LAKE, LLC (USA)

(USA)

(Consolidated with Cases No.

EXP/399/ICANN/16

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (FRANCE) vs/ EXCELLENT FIRST LIMITED (CAYMAN ISLANDS)

and

EXP/400/ICANN/17

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (FRANCE) vs/ SPRING REGISTRY LIMITED (GIBRALTAR))

This document is a copy of the Expert Determination rendered in conformity with the New gTLD Dispute Resolution Procedure as provided in Module 3 of the gTLD Applicant Guidebook from ICANN and the ICC Rules for Expertise.

INTERNATIONAL CENTRE FOR EXPERTISE
INTERNATIONAL CHAMBER OF COMMERCE

NEW GENERIC TOP-LEVEL DOMAIN NAMES (« gTLD »)
DISPUTE RESOLUTION PROCEDURE

EXP/395/ICANN/12
(consolidated with EXP/399/ICANN/16 & EXP/400/ICANN/17)

BETWEEN

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (France)

Objector

AND

CORN LAKE, LLC (USA)

Applicant

EXPERT DETERMINATION

BEFORE

Mr. Tim Portwood

Expert Panel

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

Abbreviation	Definition
ACC	Association of Corporate Counsel
Applicant	Corn Lake LLC
Applicant Additional Written Statement	The Additional Written Statement submitted by Applicant on 6 September 2013
Application	The new gTLD application by Applicant ".Charity", application ID: 1-1384-49318
Centre	The International Centre for Expertise of the International Chamber of Commerce
Community Objection	An objection to a gTLD application falling with the definition of "Community Objection" in section 3.2.1 of Module 3 of the Guidebook (and also contained in Article 2(e)(iv) of the Procedure)
Costs	As per the meaning set out in Article 14(a) of the Procedure
Expert	Mr. Tim Portwood
Expert Panel	The expert panel comprising the Expert.
GAC	ICANN's Governmental Advisory Committee
Guidebook	The gTLD Applicant Guidebook issued by ICANN (version 2012-04-06)
ICC Practice Note	The ICC Practice Note on the Administration of Cases under the Procedure

IO or Objector	The Independent Objector (Prof. Alain Pellet)
IO Additional Written Statement	The Additional Written Statement submitted by IO on 22 August 2013
Objection	The Objection Form dated 12 March 2013 transmitted by IO to the Centre on 13 March 2013 by email
Parties	The IO and the Applicant
Party	The IO or the Applicant as the case may be
Procedure	The New gTLD Dispute Resolution Procedure issued by ICANN as the Attachment to Module 3 of the Guidebook
Response	The Response (as per the meaning set out in Article 11(b) of the Procedure) submitted by Applicant on 23 June 2013
Rules	The Rules for Expertise of the International Chamber of Commerce (in force as from 1 January 2003)

1. THE PARTIES

1. IO:

PROF. ALAIN PELLET, Independent Objector, an individual residing at:

Contact Information Redacted

2. IO is represented in this Expert Determination proceeding by:

Ms Héloïse Bajer-Pellet
Contact Information Redacted

Mr. Daniel Müller
Contact Information Redacted

Mr. Phon van den Biesen
Contact Information Redacted

Mr. Sam Worsworth
Contact Information Redacted

3. Applicant:

CORN LAKE, LLC, a company incorporated under the laws of the State of Delaware, USA, with offices at:

Corn Lake, LLC
Contact Information Redacted

4. Applicant is represented in this Expert Determination proceeding by:

Mr. John M. Genga and Mr. Don C. Moody
The IP & Technology Legal Group, P.C.
Contact Information Redacted

2. THE EXPERT PANEL

5. On 4 July 2013 and pursuant to Article 3(3) of Appendix 1 to the Rules, the Chairman of the Standing Committee appointed Mr. Tim Portwood as the Expert. In accordance with Article 13 of the Procedure, the Expert is the sole member of the Expert Panel.

6. On 2nd August 2013, the Centre acknowledged receipt of payment of the Parties' respective shares of the advance payment of the estimated Costs and confirmed the full constitution of the Expert Panel.

7. The Expert's contact details are as follows:

Mr. Tim Portwood
Contact Information Redacted

3. SUMMARY OF THE EXPERT DETERMINATION PROCEEDING

8. The present Expert Determination proceeding concerns IO's Community Objection to Applicant's Application for the new gTLD ".Charity".

9. The Expert Determination is governed by and has been conducted in accordance with the Procedure and the Rules, supplemented by the ICC Practice Note.

10. IO transmitted to the Centre its Objection on 13 March 2013.

11. On 28 March 2013, the Centre informed IO that it had conducted the administrative review of the Objection pursuant to Article 9 of the Procedure and confirmed that the Objection is in compliance with Articles 5 to 8 of the Procedure and with the Rules. The Objection was therefore registered for processing under Article 9(b) of the Procedure.

12. The Centre wrote to the Parties on 12 April 2013 informing them that the Centre was considering consolidating the Objection with two other cases, namely EXP/399/ICANN/16 – a Community Objection filed by IO against an application by Excellent First Limited (Cayman Islands) for a new gTLD ".慈善 (Charity)" – and EXP/400/ICANN/17 – Community Objection filed by IO against an application by Spring Registry Limited (Gibraltar) for a new gTLD ".Charity".

13. On 7 May 2013, the Centre informed the Parties that it had decided to consolidate the present case with the two other above-referenced cases.

14. On 6 June 2013, Applicant filed with the Centre by email a Response form which failed to comply with Article 11(e) of the Procedure. Subsequently, on 23 June 2013, Applicant filed with the Centre by email its amended Response, the non-compliance with Article 11(e) of the Procedure having been remedied.

15. The Chairman of the Standing Committee having appointed the Expert on 4 July 2013, on 2nd August 2013, the Centre confirmed to the Parties the full constitution of the Expert Panel (comprising the Expert as sole member). On the same day, the Centre forwarded the file to the Expert Panel.

16. On 2nd August 2013, IO wrote to the Expert Panel requesting leave to file an Additional Written Statement.

17. On 8 August 2013, Applicant wrote to the Expert Panel objecting to IO's request for leave.

18. On 9 August 2013, having considered the Parties' submissions, the Expert Panel wrote to the Parties informing them of its view that it would be assisted by a second round of written submissions and inviting the Parties each to submit an Additional Written Statement in accordance with the following timetable: IO to file its Additional Written Submission on or before 22 August 2013 and Applicant to file its Additional Written Submission on or before 2nd September 2013.

19. On 10 August 2013, IO wrote to the Expert Panel requesting an extension of two days to the timetable for the Additional Written Submissions.

20. On 11 August 2013, Applicant wrote to the Expert Panel stating that it had no objection to IO's requests for a 2 day extension to the timetable.

21. On 13 August 2013, the Expert Panel granted IO's request, extending the deadline for the filing of IO's Additional Written Submission to 24 August 2013 and the deadline for the filing of Applicant's Additional Written Submission to 4 September 2013.

22. On 15 August 2013, Applicant requested a further extension of 2 days (i.e., 6 September 2013) for the filing of its Additional Written Statement to which IO indicated on the same day that it had no objection.

23. On 22 August 2013, IO filed by email its Additional Written Statement.

24. On 22 August 2013 the Expert Panel acknowledged receipt of IO's Additional Written Statement and confirmed that the deadline for the filing by Applicant of its Additional Written Submission was 6 September 2013.

25. On 6 September 2013, Applicant filed by email its Additional Written Statement.

26. No hearing took place.

27. The Expert Panel submitted the draft Expert Determination to the Centre for scrutiny under Article 21(b) of the Procedure within the time limit contained in Article 21(a) of the Procedure.

28. In accordance with Article 5(a) of the Procedure, the language of the proceedings is English.

29. In accordance with Article 6(a) of the Procedure, all communications by the Parties with the Centre and the Expert Panel were submitted electronically.

30. Pursuant to Article 4(d) of the Procedure, the place of the proceedings is Paris, France.

4. Issues to be Determined by the Expert Panel

4.1. IO's Impartiality and Independence

4.1.1. IO's Position

31. IO confirms that he is acting exclusively in the best interests of the public who uses the global internet and not in accordance with what he himself might prefer or with self-interest[1].

4.1.2. Applicant's Position

32. Applicant argues that IO has overstepped his role as an independent objector by making submissions which attack Applicant's (and its parent's) philosophy for an open internet and which threaten freedom of expression and by ignoring the protective mechanisms required by ICANN, those added voluntarily by Applicant (and its parent) and the new safeguards recently implemented by ICANN based on the GAC's Beijing comments[2]. Applicant points out also that IO has devoted the bulk of his efforts objecting to gTLDs applied for by Applicant's parent company in objections that lack merit. Applicant suggests in conclusion that IO is acting on the basis of what he wants for the internet and argues that this is not a basis for upholding the Objection[3].

[1] IO Additional Written Statement, para. 2.

[2] Applicant Additional Written Statement, p. 3.

[3] Response, page 9; Applicant Additional Written Statement, pp. 2-3.

4.2. IO's Standing

4.2.1. IO's Position

33. Relying upon section 3.2.5 of the Guidebook, IO denies that he has to prove that he is acting "on behalf of a 'clearly delineated community'" with which the applied-for string is strongly associated[4].

34. IO argues further that an independent objector has *ipso facto* standing in the sense of section 3.2.2 of the Guidebook, the regular standing requirements for making a Community objection being expressly disposed of by section 3.2.5 of the Guidebook in the case of objections made by an independent objector[5].

35. According to IO, under section 3.2.5 of the Guidebook, the only standing requirement for an independent objector to make a Community objection is the existence of "at least one comment in opposition to the application … made in the public sphere"[6].

36. IO points out that opposition comments to the Application have been made by, *inter alia*, the Charity Commission for England and Wales, the National Council for Voluntary Organizations and the Association of Charitable Foundations[7]. The standing requirement for IO has therefore been met, even if Applicant contests those comments[8].

4.2.2. Applicant's Position

37. Applicant maintains that independent objectors are authorized by ICANN to file Community objections only "against 'highly objectionable' gTLD applications to which no objection has been filed" referencing section 3.2.5 of the Guidebook[9].

[4] IO Additional Written Statement, para. 3.

[5] IO Additional Written Statement, para. 5.

[6] Ibid.

[7] Objection, para. 27.

[8] IO Additional Written Statement, para. 5.

[9] Response, p. 6.

38. Applicant accepts that the Guidebook grants independent objectors standing to make Community objections without fulfilling the regular standing requirements for such objections (again referencing section 3.2.5 of the Guidebook)[10]. Applicant argues further, however, citing section 3.2.2.4 of the Guidebook, that an independent objector making a Community objection must nevertheless "act on behalf of a 'clearly delineated community'"[11] and that that community must be strongly associated with the applied-for gTLD string[12].

39. Applicant submits that IO neither acts on behalf of a clearly delineated community because no "charity community" exists (as shown by the absence of any objections to the Application from any person from that "community") nor has shown any strong association between the generic term "charity" and that supposed community, the word "charity" describing a subject and not a community[13].

40. Applicant concludes that IO lacks standing to make the Community objection.

4.3. The Community Objection

41. IO's objection is a Community Objection to Applicant's Application of ".Charity" as a new gTLD.

42. The Expert Panel is therefore to determine whether there is substantial opposition to the Application from a significant portion of the community to which the gTLD string ".Charity" may be explicitly or implicitly targeted (Article 2(e)(iv) of the Procedure).

43. Under section 3.5.4 of Module 3 of the Guidebook, the Expert Panel must be satisfied that IO had proven that (i) the community invoked by IO is a clearly delineated community; (ii) community opposition to the Application is substantial; (iii) there is a strong association between the community invoked and the applied-for gTLD string (".Charity"); and (iv) the Application creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted.

[10] Ibid.

[11] Response, pp. 6-7.

[12] Response, p. 7.

[13] Ibid.

4.3.1. IO's Position

44. According to IO, an objector making a Community Objection must satisfy four tests under section 3.5.4 of the Guidebook[14]. IO states these four tests as: (a) a Community test, namely that the community invoked by the objector is a clearly delineated community; (b) a Substantial opposition test, namely that community opposition to the application is substantial; (c) a Targeting test, namely that there is a strong association between the community invoked and the applied-for gTLD string; and (d) a Detriment test, namely that the application creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted[15].

45. IO argues that the four tests are met. He submits that the applied-for gTLD string ".Charity" targets the charity sector such that the Targeting test is satisfied, even though the Application has not been framed as a community based TLD for the benefit of the charity community[16]. IO states that the charity sector constitutes a clearly delineated community in the sense of the Guidebook, thereby fulfilling the Community test. IO claims that the opposition to the Application is substantial, meaning that the Substantial opposition test is met[17]. Finally, IO pleads that the Application creates a likelihood of material detriment to the rights and legitimate interests of the charity community, fulfilling the Detriment test[18].

46. IO points out that the Guidebook does not limit Community Objections to applications for a new gTLD string made as a community gTLD[19], referring to section 1.2.3.2 of the Guidebook: "All applicants should understand that a formal 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"[20]. The Applicant's own purposes in making the Application, its own philosophy of how the internet should operate and its own understanding of the intent of ICANN in adopting the new gTLD program cannot prevail over the safeguards incorporated into the Guidebook. Those safeguards include the dispute resolution

[14] Objection, para. 8.

[15] Ibid.

[16] Objection, para. 11.

[17] Objection, para. 21.

[18] Objection, para. 46.

[19] IO Additional Written Submission, para. 7.

[20] IO Additional Written Statement, para. 8.

procedure such that a successful objection by an independent objector on any ground cannot be an unwarranted violation of the fundamental rights of freedom of expression[21].

4.3.1.1. *The Community Test*

47. IO's position is that the Community test in the Guidebook does not require that the gTLD string describes a clearly delineated community (which would render the Targeting Test otiose) but that there exists a community identified by the objector comprising a group of persons clearly delineated from others including internet users in general[22].

48. According to IO, the community in question is the charity sector[23], comprising all charitable institutions, including those that are specifically registered or regulated in some form in the states where they operate such that they must be not for profit institutions[24].

49. IO points out that the Guidebook does not provide a clear definition of the term "community". Instead, the Guidebook refers to a non-exhaustive list of factors to which the Expert Panel may refer including the recognition of the community at a local/global level, the level of formal boundaries, the length of existence, the global distribution, or the size of the community[25].

50. For IO, the distinctive element of a community is the commonality of certain characteristics, whatever they might be[26].

51. The common characteristics of the persons comprising the charity sector identified by IO are such persons' "charitable aims", "often the status of a not for profit institution", exemption from a range of regulatory requirements applicable to for-profit entities and funding through donations or public money[27].

[21] IO Additional Written Submission, paras 8 & 9.

[22] Objection, para. 18; IO Additional Written Submission, paras 10 to 15.

[23] Objection, para. 9.

[24] Objection, para. 11.

[25] Objection, para. 15 referencing section 3.5.4 of the Guidebook.

[26] Objection, para. 16.

[27] Objection para. 20.

52. Referring to Evaluation question No.20 of the Guidebook, Attachment to Module 2, IO argues that a relevant criterion is whether the group of persons comprising the community can be clearly delineated from the others – including internet users in general[28]. Recognition of the community as such (by its members and others) is an important factor in this regard[29].

53. IO points out that the charity sector is delineated as a recognizable community, distinct from others by both its members and the public, referring to public comments made on the community ground point[30].

54. IO points out that charities and charitable organizations (i.e., the charity sector) are included in the "millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need" explicitly targeted by the Applicant[31].

55. IO accepts that the charity sector is not an organized community with an entity dedicated to the community and its activities, but argues that the meaning of community in the Guidebook is not limited to organized communities and covers less structured communities, like those based on a common place of origin or a common language or a common activity or common set of goals or interests or values[32] and refers to the 2007 ICANN Final Report which confirms that "community should be interpreted broadly and will include, for example, an economic sector, a cultural community, or a linguistic community"[33].

56. IO underlines that his position is confirmed by the Advice contained in the GAC's Beijing Communiqué dated 11 April 2013[34] which considered the charity community as a market sector delineated by clear and/or regulated entry requirements on account of the level of implied trust from consumers and risk of consumer harm associated with its activities[35]. The GAC included ".Charity" in its list of sensitive strings necessitating safeguard measures.

[28] Objection, para. 18.

[29] Ibid.

[30] Objection, para. 20 ; IO Additional Written Statement, para. 16.

[31] Objection, para. 19.

[32] Objection, para. 21.

[33] Objection, para. 17.

[34] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf -Annex 1 to IO Additional Written Statement.

[35] IO Additional Written Statement, para. 17.

4.3.1.2. The Targeting Test

57. IO argues that the ".Charity" string implicitly targets the charity community (comprising charities and charitable organizations)[36] and that therefore the Targeting test is met[37].

58. IO refers to Implementation Guideline P of the 2007 ICANN Final Report which indicates that "implicitly targeting means that the objector makes an assumption of targeting or that the objector believes there may be confusion by users over its intended use". The focus of the test is not what the Applicant intends but is what the average internet user perceives and expects from the string[38]. Similarly, the test is not about what the Application targets but is about what the string itself targets[39]

59. IO notes that in the Application, Applicant explicitly targets "the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need"[40]. According to IO, that explicit target includes charities and charitable organizations[41]. The charity community is therefore implicitly targeted by the string[42].

60. IO refers also to one of the dictionary definitions of the word "charity" which indicates that it is generally associated in the public mind with giving for what is seen as a good cause and likewise with not for profit institutions that are directed to some form of charitable outcome[43]. IO adds that simply because the word bears several meanings, this does not preclude the string from having a strong association with one of those meanings if the general public is likely to make that association[44].

[36] Objection, para. 11.

[37] Objection, paras 9 and 14.

[38] Objection, para. 13.

[39] IO Additional Written Statement, para. 18.

[40] Objection, para. 11.

[41] Ibid.

[42] Objection, para. 13.

[43] Ibid referencing the definition of « charity » as « an organization set up to provide help and raise moneyfor those in need » - http://oxforddictionaries.com./definition/english/charity.

[44] IO Additional Written Statement, para. 18.

61. IO concludes that according to Applicant's own statements and the general use of the term "charity" by the public, there is a strong association between the charity sector and ".Charity"[45].

4.3.1.3. *The Substantial Opposition Test*

62. According to IO, the test whether there is "substantial opposition within the community" to the Application is largely casuistic[46].

63. IO refers to the non-exhaustive list of factors in the Guidebook which an Expert Panel may use to identify substantial opposition to the Application[47] noting that the factors are more useful in cases of well-organized and structured communities than in cases like the present of communities lacking organizational structures or clear representation[48].

64. IO argues that a mere numerical criterion – the number of voiced oppositions to the Application – was not the intent of the Guidebook, the word "substantial" meaning not simply a large number but also something of "considerable importance" or "considerable worth"[49]. According to IO, therefore, the material content of comments and oppositions and the rights and interests of those expressing those comments and oppositions must be taken into account[50].

65. IO identifies opposition comments having been posted on the public comments website by the Charity Commission for England and Wales, the National Council for Voluntary Organizations and the Association of Charitable Foundations, the first being the regulator of charities in England and Wales and the last representing a membership of some 330 charitable trusts and foundations in England and Wales[51]. IO refers also to the Australian member of the GAC having issued an Early Warning regarding ".Charity"[52]. According to IO, the common underlying concern of such opposition comments and Early Warning is the potential harm to the system of trust on which

[45] Objection, para. 14.

[46] Objection, para. 22.

[47] Objection, para. 23.

[48] Objection, para. 24.

[49] Objection, para. 25.

[50] Objection, para. 25.

[51] Objection, para. 27.

[52] Ibid.

charities and charitable are largely dependent that would be caused in the absence of sufficient protection mechanisms such as strict eligibility criteria for users of the string[53].

66. IO admits that the opposition to the Application has largely emanated from the UK and Australia but argues that the concerns that have been voiced are substantively substantial, are "without doubt ... of much more general application"[54] and include the views of one or more governments (referencing section 1.1.2.4 of the Guidebook)[55].

4.3.1.4. *The Detriment Test*

67. IO emphasizes that the Detriment test requires a finding of "a likelihood of detriment"[56] and not of actual detriment – which would be anathema, the string not yet having been put into use[57] – the idea of requiring a finding of actual detriment having been abandoned during the *travaux* of ICANN[58].

68. According to IO, the likelihood of detriment must be created by the Application and therefore must take into account the Applicant and the security protection for user and community interests that Applicant has proposed or intends to adopt[59].

69. IO underlines that the likelihood of detriment must be to the rights or legitimate interests of the community or to users more widely, referring to Implementation Guideline P[60]. He refers to the guidance in the Guidebook and summarizes that detriment may include harm to the reputation of the community, interference with the community's core activities, economic or other concrete damage to the community or significant portions of the community[61].

70. IO points out that the Expert Panel may take into account a variety of factors, including the dependence of the community on the DNS for its core activities, the intended use of the gTLD as stated in the Application, the importance of the rights and interests

[53] Objection, paras 27 to 31 ; IO Additional Written Statement, para. 20.

[54] Objection, para. 33.

[55] Objection para. 32.

[56] Objection, para. 34.

[57] IO Additional Written Statement, para. 22.

[58] IO Additional Written Statement, para. 22.

[59] Objection para. 36.

[60] Objection, para. 34.

[61] Objection, para. 35.

exposed for the community targeted and for the public more generally[62] and whether the Applicant intends acting in accordance with those rights and interests[63].

71. IO argues, in line with the GAC's Beijing Communiqué of 11 April 2013[64], that the charity sector relies on public trust without which its gift and other funding would be threatened. Public regulation exists in many jurisdictions precisely to protect and nurture that trust[65]. Administration of the ".Charity" string outside such or similar protections and safeguards could, according to IO, citing the Charity Commission of England and Wales, lead to "scope for confusion, misunderstanding and, perhaps, deliberate abuse, resulting in turn in significant damage to charities if public support dropped as a result"[66].

72. IO asserts that the Application does not address the specific needs of the charity community and points to three factors that demonstrate a likelihood of detriment to that community: (i) Applicant has not framed the Application as a community based gTLD, thereby avoiding certain consequences for the evaluation of the Application and the terms (such as user registration requirements) under which the gTLD would be operated[67]; (ii) no registrant eligibility criteria are proposed for the string, Applicant preferring to address abuse if it occurs, such that the needs and requirements of the charity community would not be addressed in a preventive manner[68] and it being up to Applicant (and not IO) to enumerate its Application with sufficient specificity to meet the required tests[69]; and (iii) the security mechanisms proposed in the Application to react to abuse are unspecific, often left to the discretion of the Applicant and its parent company and largely identical to the mechanisms proposed by Applicant's sister companies for strings with different features such as ".Creditcard"[70].

73. IO concludes that Applicant, like its ultimate parent, continues to affirm a pro-open registry philosophy for new gTLDs that fails to address the specific characteristics of the ".Charity" string, including the need to protect public trust in charities and

[62] Objection para. 35.

[63] Objection, para. 36.

[64] IO Additional Written Statement, para. 24 and Annex 1 thereto.

[65] Objection, paras. 37 & 38.

[66] Objection, para. 39.

[67] Objection, para. 42.

[68] Objection, para. 43.

[69] IO Additional Written Statement, para. 25.

[70] Objection, para. 45.

charitable organisations being the community implicitly targeted by the string, and that is evidenced by the challenge to the safeguard measures advised by the GAC made by Applicant's ultimate parent[71].

4.3.2. *Applicant's Position*

74. Relying on section 3.5.4 of the Guidebook, Applicant states that an objector making a Community objection must satisfy four tests to succeed, namely, the Community test, the Targeting test, the Substantial Opposition test and the Detriment test[72]. It points out that failure on any one test compels denial of the objection[73].

75. Applicant's position is that none of the tests is met by IO[74].

4.3.2.1. *The Community Test*

76. Applicant notes that the standing requirement and the substantive tests for a Community objection both impose on an independent objector a showing that a "clearly delineated community" exists[75]. In order to satisfy the general rule that all parts of different tests must have an operative meaning, Applicant argues that ICANN must have intended the substantive "Community test" to be "a more stringent test … than for standing"[76].

77. Applicant looks to ICANN's purpose for the Community objections and cites a public comment from eNOM of 21 July 2009 transcribed into ICANN's Summary Report and Analysis of Public Comment, 2 October 2009 (http://archive.icann.org/en/topics/new-gtlds/agve-analysis-public-comments-04oct09-en.pdf) at p.19 where eNOM stated the objective of Community objections being "to prevent the misappropriation of a string that uniquely or nearly uniquely identifies a well-established and closely connected group of people or organizations"[77]. Applicant argues that the intent behind the Community test set out in the Guidebook is therefore that the string must itself describe

[71] IO Additional Written Statement, para. 27.

[72] Response, p. 7.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Ibid.

or "clearly delineate" a "community"[78]. Referring to section 4.2.3 of the Guidebook, Applicant submits that "a community must have more 'cohesion than a mere communality of interest'"[79].

78. Relying on section 3.5.4 of the Guidebook, Applicant identifies five factors that an objector must prove to show that the Community test is met: (i) public recognition of the group as a community at a local and/or global level; (ii) formal boundaries around the community, such as who specifically forms the community; (iii) how long the community has existed; (iv) the community's global distribution; and (v) how many people or entities comprise the community[80].

79. Applicant argues that IO has failed to provide evidence of any of these factors.

80. Applicant states that IO's definition of the charity community as "millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need" which includes "charities and charitable organizations" has no boundaries and potentially includes "planet Earth"[81].

81. Although IO has extracted a subset of "charities and charitable institutions", Applicant argues that IO has failed to delineate such subset as a community as Applicant says IO has admitted when he states in his Objection (para. 21) that the "charitable community ... [is] not institutionalized and straddles the border between different stakeholders of the community of charitable organizations"[82]. Applicant submits that the community standard was crafted by ICANN to avoid legitimate uses of generic terms, such as charity, being blocked by the objection process[83].

82. Applicant points out that the word "charity" has many meanings and represents a subject – IO having failed to show that the public recognizes "charity" as a "community"[84].

83. Even if the "community" in question were "charitable institutions", Applicant argues that IO still fails to discharge the burden of proof imposed by the Community test not

[78] Applicant Additional Written Response, p. 3.

[79] Response, p. 7.

[80] Applicant Additional Written Response, p. 3.

[81] Response, p. 8.

[82] Ibid.

[83] Ibid.

[84] Response, p. 9.

having defined "charitable institution" – itself a generic and widely-applicable term[85]. At best, "charitable institutions" constitutes a "loosely delineated" community: not the required "clearly delineated" one.

84. In response to IO's reliance on the GAC comments, Applicant states that the GAC Beijing Advice does not in fact view ".Charity" as a string delineating a community but merely considers that string is one of many "sensitive strings" for which possible additional safeguards may be necessary[86].

85. In addition to IO having failed to discharge the burden of proving that "charity" constitutes a clearly delineated community, Applicant claims that the Objection would, if successful, stifle free expression and discourse and thus undermine the purpose of ICANN's new gTLD program as well as Applicant's open-internet philosophy[87].

4.3.3. The Substantial Opposition Test

86. Applicant refers to section 3.5.4 of the Guidelines and argues that IO must prove substantial opposition to the Application from the community on whose behalf IO purports to speak. Applicant extracts from that Article six factors to be taken into account: (i) the number of expressions of opposition; (ii) the representative nature of those expression opposition; (iii) the stature or weight of the opposition; (iv) the distribution or diversity of opposition within the community; (v) the defence of the community in other contexts by those expressing opposition; and (vi) costs incurred in expressing opposition[88].

87. Applicant points out that IO relies upon only three of the seven public comments made to ICANN in respect of the Application as well as the Early Warning by the Australian member of GAC[89]. Those three public comments all come from the same jurisdiction – the UK. Two use the same language and thus express the same concern[90]. The other is limited to general concern about consumer confusion and abuse if the string is administered improperly which suggests a need to examine Applicant's safeguard

[85] Applicant's Additional Written Statement, p.3.

[86] Applicant's Additional Written Statement, pp. 4 & 7-9.

[87] Response, p. 9.

[88] Response, p. 9.

[89] Ibid.

[90] Ibid.

measures but not to block the Application[91]. Not one comment relates to Applicant itself[92].

88. Applicant summarizes the seven public comments about the Application as emanating almost entirely from the UK and being limited to two concerns: (i) that ".Charity" should be run by a not-for-profit organization with which IO disagrees; and (ii) that ".Charity" should be a community-based TLD, a requirement not imposed by ICANN[93].

89. Applicant concludes that IO has failed to adduce anything more than scant evidence of opposition which cannot be characterized as substantial opposition from a significant portion of the global "charity community". What that evidence of opposition might do is to enable IO to have standing to object, but falls short of satisfying the Substantial opposition test[94].

4.3.4. *The Targeting Test*

90. Applicant relies on section 3.5.4 of the Guidebook and argues that IO must prove a "strong association" between the applied-for string and the community he invokes by relying on statements in the Application, public statements by the Applicant and public associations between the string and the community[95].

91. Applicant criticizes IO for having failed to take any account of what the Applicant targets[96] and points out that in its Application it is targeting a wide variety of users – "millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach, and the benevolent care of those in need (relying on the Declaration of Mr. Jonathan Nevett, the founder and Executive Vice President of Applicant's parent company): not a discrete set which would run contrary to its parent's internet philosophy[97].

92. Applicant argues that IO has failed to present evidence that the public strongly associates the word "charity" with any delineated community – all that IO has done,

[91] Ibid.

[92] Response, p. 10.

[93] Response, p. 9.

[94] Applicant Additional Written Statement, p. 5.

[95] Response, p. 10.

[96] Applicant Additional Written Statement, p. 4.

[97] Response, pp. 10 – 11.

according to Applicant, is to ignore the generic nature of the string[98] and to identify users who may have an interest in the subject of charity. That, for Applicant, is not targeting within the meaning of the Guidebook[99].

4.3.5. *Detriment Test*

93. According to Applicant who relies on section 3.5.4 of the Guidebook, the detriment test requires an independent objector to prove "likelihood" of "material detriment" which in turn calls for proof of (i) the nature and extent of potential damage to the "community" or its reputation from Applicant's operation of the string; (ii) evidence that Applicant does not intend to act consistently with the interests of that "community"; (iii) interference with the core activities of that "community" by Applicant's operation of the string; (iv) the extent to which the "community" depends on the DNS for core activities; and (v) the level of certainty that detrimental outcomes will occur[100].

94. Applicant disagrees with IO regarding the need of an objector to provide evidentiary support for its arguments. Whilst IO argues that the Guidebook does not require such support (given the prospective nature of the Detriment test – likelihood of detriment –), Applicant relies upon Implementation Guideline P, Final Report on the Introduction of New Generic Top-Level Domains, 8 August 2007 where it is stated that "the objector must provide sufficient evidence to allow the panel to determine that there would be a likelihood of detriment to the rights or legitimate interests of the community or to users more widely" adding that IO has relied itself upon those Guidelines (albeit on the different issue of standing)[101].

95. Applicant argues that IO has failed on all points – having raised just one point: namely that if persons other than recognized charitable organizations can use a ".Charity" TLD, abuse and harm may potentially occur[102].

96. Applicant argues that because it has not applied for a community based gTLD is not proof of harm since the ICANN rules and process permit applications such as the Application[103].

[98] Applicant Additional Written Statement, p. 4.

[99] Response, page 11.

[100] Response, p. 11.

[101] Applicant Additional Written Statement, p. 6.

[102] Response, p. 12.

97. Applicant asserts that it shares IO's desire that the ".Charity" string be used for the creation of a trusted place of information about charitable activities – hence the Application's compliance with the 14 ICANN protections, the additional 8 safeguards Applicant agrees to put in place[104] and the four further measures Applicant says it will implement due to the sensitivity of the string following the GAC Beijing Advice[105]. Applicant argues that IO has simply ignored such undertakings[106]

98. Applicant criticizes IO's suggestion of a need for registration eligibility criteria because IO has failed to specify what such criteria would be[107]. Applicant argues further that the Guidebook does not require the onerous registration restrictions as opposed to safeguards suggested by IO[108] and points out that IO's reliance on the GAC Beijing Advice in this regard is misplaced since the ICANN Board is not obliged to accept such Advice (and indeed has not done so to-date)[109].

99. Applicant adds that IO has failed to make an assessment of the certainty of harm occurring[110].

100. Finally Applicant argues that the effect of upholding the Application would "eviscerate free speech and competition" and "subvert ICANN's goals"[111] and that IO's arguments on the Detriment test boil down to a disagreement with Applicant's "open registry" approach[112].

[103] Response, p. 12.

[104] Response, p. 12.

[105] Applicant Additional Written Statment, p. 5.

[106] Applicant Additional Written Statement, p. 5.

[107] Response, p. 12.

[108] Applicant Additional Written Statement, p. 7.

[109] Applicant Additional Written Statement, p. 7.

[110] Response, p. 12.

[111] Response, p. 13.

[112] Applicant Additional Written Statement, p. 6.

5. EXPERT PANEL'S DETERMINATION

5.1. IO's Independence and Impartiality

101. Section 3.2.5 of the Guidebook requires that independent objectors *"be and remain independent and unaffiliated with any of the gTLD applicants"*. It states further that an independent objector *"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"*.

102. The mere statement by Applicant that IO may have devoted "the bulk" of his objections to applications (including the Application) filed by Applicant's parent is not in the view of the Expert Panel a basis in and of itself to question IO's independence and impartiality under section 3.2.5 of the Guidebook. The question whether those objections have or lack merit (the latter being according to Applicant an indication of bias) is, in any event, beyond the remit of this Expert Determination. The Expert Panel has no evidence before it that gives reason to challenge IO's confirmation that he is acting exclusively in the best interests of the public who use the global internet.

103. The Expert Panel would point out that the present Application has been consolidated with two other applications (EXP/399/ICANN/16 and EXP/400/ICANN/17) in which IO has objected to applications made by other applicants that the Applicant. The existence of these other objections by IO is an indicator that IO is not acting out of any particular bias or targeting of Applicant.

104. The Expert Panel rejects, therefore, Applicant's challenge to IO's Independence and Impartiality.

5.2. IO's Standing

105. The "mandate and scope" for independent objectors are set out in section 3.2.5 of the Guidebook and comprise three elements: (i) *"The IO is granted standing to file objections on th[e] enumerated grounds, notwithstanding the regular standing requirements for such objections …"*; (ii) *"The IO may file objections against "highly objectionable" gTLD applications to which no objection has been filed"*; and (iii) *"the IO shall not object to an application unless at least one comment in opposition to the application is made in the public sphere"*.

106. Only one of these elements, the first cited above, is described in terms of "standing". This is how IO reads the Guidebook, making no reference to the second element that the Application is "highly objectionable" and treating the third, at least one publicly stated opposition to the Application, as a condition to an objection by an independent objector being admissible. Applicant on the other hands treats all three elements as going to "standing" but only develops argument on the first, accepting that the third element has been met and merely citing the second.

107. Given the phraseology chosen by the authors of the Guidebook, the Expert Panel prefers IO's view and considers that there is only one criterion for the standing of an IO to make a Community Objection: namely that he or she is an independent objector within the meaning of the Guidebook, as is the case here, to whom the regular standing requirements for the particular objection do not apply.

108. The third element is not, strictly speaking, therefore, a requirement of standing, but operates as a condition of admissibility for any objection by an independent objector. It is not disputed that the condition is fulfilled in this case.

109. The drafting of the second element is different from the first (phrased in terms of standing) and the third (phrased in terms of a negative condition) and uses permissive language: "*may file objections* ...". The Guidebook drafters' decision not to craft this element as a standing requirement or negative condition distinguishes it from the first and third. That choice of different language should be given meaning.

110. That meaning can be drawn from the purpose behind the introduction of independent objectors in the new gTLD dispute resolution procedure as stated by ICANN in its Explanatory Memorandum on the Description of Independent Objector for New gTLD Dispute Resolution Process dated 18 February 2009[113]. The role of independent objectors is stated to be the answer to the question "what will be done if there is an application for a highly objectionable name but there are no objections within the process?". The Explanatory Memorandum uses various formulations for what is meant by "highly objectionable" including "clearly objectionable", "controversial applications", "highly controversial strings", "valid objections" and "strings considered objectionable across many jurisdictions". Whilst the formulation varies, therefore, the purpose is clear: to have a means of dealing with applications which raise issues that should be determined within the dispute resolution procedure but which, for whatever

[113] http://www.newgtlds.icann.org/en/about/historical-documentation/matrix-agb-v2.pdf

reason, have not attracted an objection by a person satisfying the regular standing criteria.

111. That purpose raises the more important question for the Expert Panel as to whether satisfaction of the "highly objectionable" criterion is an issue for determination *in limine*, on the merits or at all. The Explanatory Memorandum is helpful. It states: "*It is anticipated that in each instance the Independent Objector would make an independent assessment as to whether an objection is warranted ... It is anticipated that the Independent Objector will have the discretion and judgment to only act in clear cases where the grounds for objection seem strong*". The Expert Panel concludes, therefore, that this second element of the mandate refers to the discretion given to the independent objector over when to act and an indicator of how that discretion should be exercised. It is not therefore a criterion of standing or admissibility of an objection.

112. The Expert Panel determines, therefore, that IO has standing to make this Objection.

5.3. The Community Objection

113. In order for his Objection to succeed, IO bears the burden of proving that four tests are met: (a) a Community test, namely that the community invoked by the objector is a clearly delineated community; (b) a Substantial opposition test, namely that community opposition to the application is substantial; (c) a Targeting test, namely that there is a strong association between the community invoked and the applied-for gTLD string; and (d) a Detriment test, namely that the application creates a likelihood of material detriment to the rights or legitimate interests of a significant of the community to which the string may be explicitly or implicitly targeted[114].

5.3.1. The Community Test

114. Pursuant to section 3.5.4 of the Guidebook, IO has the burden of proving to the Expert Panel that "*the community invoked by the objector is a clearly delineated community*".

115. The "community" in question is the one invoked by the objector – it is not the community targeted by the string, the applicant or the application.

[114] Objection, para. 8.

116. The objector in this case is IO. The community invoked by IO is "the charity sector" comprising all "charitable institutions".

117. The question for determination, therefore, is whether IO has proven to the Expert Panel that the "charity sector" comprising all "charitable institutions" constitutes a "clearly delineated community".

118. The Guidebook does not provide a definition of "clearly delineated community" but lists five factors that an Expert Panel may balance when making its determination. That list is neither exhaustive, conclusive nor imperative. None of the cited factors goes to the heart of what is a "community" but each assists in identifying a "community" when it exists: public recognition of the community, level of formal boundaries, length of existence, global distribution and number of members.

119. IO and Applicant agree that for a community to exist there must be a degree of "communality" among the members whether of "interest" or "characteristics" – although the Parties disagree as to the necessary degree. For IO "commonality of certain characteristics" is sufficient whereas for Applicant cohesion rather than just a commonality of interests is required. It seems that the difference is in fact one of degree rather than substance. The Expert Panel accepts the view in the 2007 ICANN Final Report that "community should be interpreted broadly and will include, for example, an economic sector, a cultural community, or a linguistic community". Whether the group or sector is sufficient delineated to pass the Community test is casuistic and the distinction drawn by Applicant between commonality of interest and cohesion is not particularly helpful.

120. IO states that the common characteristics of the members of the "charity sector" include their charitable aims, often status as not-for-profit institutions, often exemption from regulatory requirements applicable to for-profit entities and funding through donations or public money. Given the obviousness of each of these characteristics in the Expert Panel's view none requires the support of specific evidence to be found as facts.

121. The existence in many jurisdictions, such as the UK, of regulators of the charity sector is an indication that that sector is capable of delineation and is considered publicly to be different from others.

122. The public comments made with respect to the Application indicate that publicly the charity sector is considered to exist separately from other sectors of activity.

123. IO accepts that the "charity sector" has no clear geographical boundaries – indeed it is global – and is not structured in any way. These are factors which may be taken into account as indices of the absence of a community but are not conclusive.

124. Balancing these various factors and considerations, the Expert Panel finds that the charity sector, comprising all charitable institutions, constitutes a clearly delineated community within the meaning of section 3.5.4 of the Guidebook. The "Community test" has been satisfied by IO.

5.3.2. The Targeting Test

125. Pursuant to section 3.5.4 of the Guidebook, IO has the burden of proving "*a strong association between the applied-for gTLD string and the community*" invoked by the objector.

126. The "strong association" sometimes referred to as "targeting" that must be shown by IO to exist therefore is between the applied-for gTLD and the community invoked by IO: namely, between ".Charity" and the "charity sector".

127. The Guidebook does not define "a strong association" or "targeting" but identifies three sources of evidence that an independent objector may use to show that it exists: statements in the application, other public statements by the applicant and associations by the public. Those three factors are neither exhaustive, imperative nor conclusive.

128. Targeting may be explicit or implicit as explained in Implementation Guideline P of GNSO's Principles, Recommendations and Implementation Guidelines. Whilst that Implementation Guideline P addresses specifically the Substantial opposition test, its reference to the possibility of implicit targeting must logically apply equally to the Targeting test satisfaction of which is a pre-condition to considering whether the Substantial opposition test is met.

129. Explicit targeting is where there is a description of the intended use of the applied-for gTLD in the application; implicit targeting is when the objector makes an assumption of targeting or that the objector believes there may be confusion by users over the use of the applied-for gTLD.

130. IO presents its objection as one of implicit targeting, accepting that the term "charity" has numerous meanings like other generic terms. IO must satisfy the Expert Panel that its assumption of targeting or belief that confusion among users may occur is legitimate.

131. In the Application, Applicant states that the applied-for gTLD is aimed at "the millions of persons and organizations worldwide involved in philanthropy, humanitarian outreach and the benevolent care of those in need". The Expert Panel finds that within that statement there is an implicit reference to the "charity sector", the community invoked by IO, such that there can be a legitimate assumption on the part of IO of targeting.

132. IO relies also on one of the dictionary definitions of the word "charity" as a charitable institution. The Expert Panel finds that this definition of the word "charity" means that there would be public association of ".Charity" with the charity sector and therefore that IO has a legitimate belief that confusion over the use of the applied-for gTLD may occur.

133. The GAC Beijing Advice provides further evidence that the public would associate ".Charity" with charitable institutions – the charity sector – given the concern expressed over the sensitive nature of the applied-for gTLD string precisely because of the regulated nature of the charity sector and level of implied trust from consumers invoked by the string. Such concern implies the "strong association" required by the Targeting test.

134. Applicant's responses that its target is much broader than charitable institutions and that the word "charity" is a generic term with many other meanings than charitable institutions do not detract from the strong association between ".Charity" and the charity sector or the implicit targeting of ".Charity" to that sector. All that those responses do is to point out that other associations and other targeting may exist. It is not however for IO to satisfy the Expert Panel that the strong association or targeting identified is exclusive.

135. The Expert Panel is therefore satisfied that IO has proven that the Targeting test is satisfied.

5.3.3. *The Substantial Opposition Test*

136. Substantial opposition is not defined in the Guidebook other than to indicate that the opposition is to be to the application (as opposed to the applicant). Instead, section 3.5.4 of the Guidebook provides a list of factors which the Expert Panel may balance to determine whether substantial opposition to the Application exists. That list is neither exhaustive, imperative nor conclusive.

137. IO and Applicant disagree over the meaning of "substantial". IO argues that "substantial" may refer to the number of statements of opposition relative to the composition of the community and/or to the substantive importance or worth of the statements of opposition. Applicant considers that the factors listed in section 3.5.4 of the Guidebook focus on the number of statements of opposition.

138. A review of the factors listed in section 3.5.4 indicates that a mere numerical meaning for "substantial" would be wrong. Those factors include not only the relative number of statements of opposition but also the representative nature of those expressing opposition and the recognized weight or stature of the expressions of opposition.

139. IO relies upon public comments from the Charity Commission for England and Wales, the National Council for Voluntary Organizations, the Association of Charitable Foundations, the Australian member of the GAC (in the form of an Early Warning) and the Office of the Scottish Charitable Regulator (as part of a legal rights objection). The Charity Commission is the regulator of charities in England and Wales. The Association of Charitable Foundations represents some 330 charitable trusts and foundations in England and Wales. The National Council for Voluntary Organizations represents just under 10,000 voluntary organizations (not all charitable institutions) in the UK. The Office of the Scottish Charitable Regulator is the regulator of charities in Scotland. The Australian member of the GAC is a representative of the Australian government.

140. The Charity Commission for England and Wales, the Office of the Scottish Charitable Regulator, the Association of Charitable Foundations and the National Council for Voluntary Organizations state their opposition on the potential harm to the system of trust on which charities and charitable giving are dependent if the ".Charity" string were to be run by a for-profit organization – arguing that had the Application been made as a community-based application their concerns would be assuaged given the status requirements for a community-based Applicant. Similar concerns are expressed by the Australian member of the GAC.

141. IO refers to the other public opposition comments made to ICANN[115]. These include opposition from the Association of Corporate Counsel ("ACC") which has over 30,000 members (in-house counsel) employed by over 10,000 organizations in more than 75 countries. The Association's Not-for-profit Organizations Committee offers a collective voice to over 1,400 in-house counsel practising law in nonprofit institutions across the

[115] http://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments

globe. In addition to concerns over abuse (for which the ACC proposes two types of safeguards), the ACC points to the need for protection *"given the intimate and obvious connection between [.Charity] and our members' organizations that operate in the philanthropy field"*.

142. The Expert Panel would point out that the relative number of statements of opposition is small. Those statements come from the same or similar common law jurisdictions. These are two factors that, in the Expert Panel's view, militate against a finding that there is substantial opposition.

143. This small number of opposition statements comes from bodies that are representative of a larger number of members of the charity sector not only in jurisdictions where regulation of charitable activities is historically strong, developed and well-established but also in the case of ACC, worldwide. These are factors which militate in favour of a finding that there is substantial opposition.

144. The fact that the opposition raised by the different statements is substantively similar does not detract from the number of statements or from their representative nature or relative importance.

145. On balance, the Expert Panel is satisfied that IO has provided evidence of substantial opposition to the Application such that the Substantial opposition test is met.

5.3.4. *The Detriment Test*

146. Pursuant to section 3.5.4 of the Guidebook it is for IO to prove that the Application (or rather use of the applied-for gTLD as contemplated by the Application) creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted.

147. The test requires evidence of a likelihood of material detriment and not evidence of actual detriment – which would be impossible given the prospective nature of the objection process.

148. Evidence of a likelihood of something happening – cause and effect occurring in the future – is inherently difficult. It is no doubt for this reason that the Guidebook focuses on a variety of factors (none of which is imperative or conclusive) that IO may prove to lead to the conclusion that material detriment is likely. These factors include the dependence of the community on the DNS for its core activities, the intended use of the gTLD as stated in the Application, the importance of the rights and interests exposed

for the community and the public, and whether the Applicant intends acting in accordance with those rights and interests.

149. The various public statements of opposition to the Application are all premised on the importance of the global internet as a means of recognition and fund-raising for the charity sector. It is therefore generally accepted that the DNS is important for a core activity of the community.

150. Those public statements of opposition all focus on the need clearly to distinguish charitable organizations from for-profit enterprises in particular in public giving and fund-raising activities. They point out the absence of any limitation in the Application of the ".Charity" string to not-for-profit or charitable organizations – the stated purpose of the Applicant in the Application being to the contrary. This concern is the origin of the suggestion in many of the public statements of opposition that the ".Charity" string should be treated only as a community-based gTLD.

151. The public statements of opposition identify the rights and interests of the community and the public that are exposed to harm if the Application were to proceed as the need of the charity sector for public funding to finance its activities; the trust and confidence of the public in the charity sector that donations will be used for the stated charitable ends. They point out that those rights and interests are protected outside the internet by public regulation of recourse to public giving for charitable purposes. They and IO emphasize the need for strict registration eligibility criteria limited to persons regulated as charitable bodies or their equivalent depending upon domestic law.

152. The Expert Panel is of the view that these public statements of opposition that are echoed by IO cannot be ignored as they point to an important characteristic of the targeted community (including its existence and its activities) that would be harmed if access to the ".Charity" string were not restricted to persons (whether incorporated entities, unincorporated associations or entities, foundations or trusts) which can establish that they are a charity or a not-for-profit enterprise with charitable purposes.

153. The Application expressly avoids such a limitation and therefore the protection that the Expert Panel considers should exist stating *"we believe attempts to limit abuse by limiting registrant eligibility is unnecessarily restrictive and harms users by denying access to many legitimate registrants. Restrictions on second level domain eligibility would prevent law-abiding individuals and organizations from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD"*.

154. Applicant emphasizes the Application's compliance with the 14 ICANN protections, the additional 8 safeguards Applicant agrees to put in place and the 4 further measures that Applicant says it will implement following the GAC Beijing Advice. Those protections, safeguards and measures focus on avoiding and eradicating abuse. They do not therefore respond to the rights and interests of the charity sector community since abuse is not, *ex hypothesi*, defined in the Application in terms of those rights and interests. There is nothing in the Application, therefore, to indicate that Applicant will act in accordance with the rights and interests of the community.

155. Whilst the Expert Panel acknowledges the value of Applicant's (and its parent's) vocation for freedom of speech and competition throughout the internet, those general aims are not factors to be taken into account when assessing an objection (which focuses on the four tests that the objector must satisfy for its objection to succeed).

156. In view of the foregoing, the Expert Panel is satisfied that there is a likelihood of material detriment to the charity sector community were the Application to proceed such that the Detriment test is satisfied.

5.3.5. *Conclusion*

157. Having reviewed the Parties' submissions and supporting evidence and for the foregoing reasons, the Expert Panel upholds IO's Community Objection against the Application.

5.4. Costs of the Expert Determination

158. Article 14(e) of the Procedure provides which of the Parties shall bear the Costs.

159. The Objection has been upheld.

160. In accordance with Article 14(e) of the Procedure, the advance payment on Costs made by IO is therefore to be reimbursed.

5.5. Expert Panel's Determination

161. In light of the above and in accordance with Art. 21(d) of the Procedure, the Panel hereby renders the following Expert Determination:

i. The Objection is upheld and therefore the Independent Objector is the prevailing party.

ii. The Independent Objector is thus entitled to a refund of the advance payment of Costs by the Centre pursuant to Article 14(e) of the Procedure.

Done in Paris.

9 January 2014

Mr. Tim Portwood
Expert Panel

Attachment 9

[Ruling in consolidated SRL case]

THE INTERNATIONAL CENTRE FOR EXPERTISE OF THE

INTERNATIONAL CHAMBER OF COMMERCE

CASE No. EXP/400/ICANN/17

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR

(FRANCE)

vs/

SPRING REGISTRY LIMITED

(GIBRALTAR)

(Consolidated with Cases No.

EXP/395/ICANN/12

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (FRANCE) vs/ CORN LAKE, LLC (USA)
and

EXP/399/ICANN/16

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (FRANCE) vs/ EXCELLENT FIRST LIMITED (CAYMAN ISLANDS))

This document is a copy of the Expert Determination rendered in conformity with the New gTLD Dispute Resolution Procedure as provided in Module 3 of the gTLD Applicant Guidebook from ICANN and the ICC Rules for Expertise.

INTERNATIONAL CENTRE FOR EXPERTISE
INTERNATIONAL CHAMBER OF COMMERCE

NEW GENERIC TOP-LEVEL DOMAIN NAMES ("gTLD")
DISPUTE RESOLUTION PROCEDURE

EXP/400/ICANN/17
(consolidated with EXP/395/ICANN/12 and EXP/399/ICANN16)

BETWEEN

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (France)

Objector

AND

SPRING REGISTRY LIMITED (Gibraltar)

Applicant

EXPERT DETERMINATION

BEFORE

Mr. Tim Portwood

Expert Panel

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

Abbreviation	Definition
ACC	Association of Corporate Counsel
Applicant	Spring Registry Limited
Applicant Additional Written Statement	The Additional Written Statement submitted by Applicant on 6 September 2013
Application	The new gTLD application by Applicant ".Charity", application ID: 1-1241-87032
Centre	The International Centre for Expertise of the International Chamber of Commerce
Community Objection	An objection to a gTLD application falling with the definition of "Community Objection" in section 3.2.1 of Module 3 of the Guidebook (and also contained in Article 2(e)(iv) of the Procedure)
Costs	As per the meaning set out in Article 14(a) of the Procedure
Expert	Mr. Tim Portwood
Expert Panel	The expert panel comprising the Expert
Guidebook	The gTLD Applicant Guidebook issued by ICANN (version 2012-04-06)
ICC Practice Note	The ICC Practice Note on the Administration of Cases under the Procedure
IO or Objector	The Independent Objector (Prof. Alain Pellet)

IO Additional Written Statement	The Additional Written Statement submitted by IO on 22 August 2013
Objection	The Objection Form dated 12 March 2013 transmitted by IO to ICANN on 13 March 2013 by email
Parties	The IO and the Applicant
Party	The IO or the Applicant as the case may be
Procedure	The New gTLD Dispute Resolution Procedure issued by ICANN as the Attachment to Module 3 of the Guidebook
Response	The Response (as per the meaning set out in Article 11(b) of the Procedure) submitted by Applicant on 5 June 2010
Rules	The Rules for Expertise of the International Chamber of Commerce (in force as from 1 January 2003)

1. THE PARTIES

1. IO:

PROF. ALAIN PELLET, Independent Objector, an individual residing at:

16, avenue Alphonse de Neuville,
92380 Garches,
France.

2. IO is represented in this Expert Determination proceeding by:

Ms Héloïse Bajer-Pellet
Contact Information Redacted

Mr. Daniel Müller
Contact Information Redacted

Mr. Phon van den Biesen
Contact Information Redacted

Mr. Sam Worsworth
Contact Information Redacted

3. Applicant:

SPRING REGISTRY LIMITED, a company incorporated under the laws of Gibraltar, with offices at:

Spring Registry Limited
6A Queensway
Gibraltar, GX11 1AA

4. Applicant is represented in this Expert Determination proceeding by:

Mr. Peter Young
Contact Information Redacted

2. THE EXPERT PANEL

5. On 4 July 2013 and pursuant to Article 3(3) of Appendix 1 to the Rules, the Chairman of the Standing Committee appointed Mr. Tim Portwood as the Expert. In accordance with Article 13 of the Procedure, the Expert is the sole member of the Expert Panel.

6. On 2 August 2013, the Centre acknowledged receipt of payment of the Parties' respective shares of the advance payment of the estimated Costs and confirmed the full constitution of the Expert Panel.

7. The Expert's contact details are as follows:

Mr. Tim Portwood
Contact Information Redacted

3. SUMMARY OF THE EXPERT DETERMINATION PROCEEDING

8. The present Expert Determination proceeding concerns IO's Community Objection to Applicant's application for the new gTLD ".Charity".

9. The Expert Determination is governed by and has been conducted in accordance with the Procedure and the Rules, supplemented by the ICC Practice Note.

10. IO transmitted to the Centre its Objection on 13 March 2013.

11. On 28 March 2013, the Centre informed IO that it had conducted the administrative review of the Objection pursuant to Article 9 of the Procedure and confirmed that the Objection was in compliance with Articles 5 to 8 of the Procedure and with the Rules. The Objection was therefore registered for processing under Article 9(b) of the Procedure.

12. The Centre wrote to the Parties on 12 April 2013 informing them that the Centre was considering consolidating the Objection with two other cases, namely EXP/395/ICANN/12 – a Community Objection filed by IO against an application by Corn Lake, LLC (USA) for new gTLD ".charity" – and EXP/399/ICANN/16 – Community Objection filed by IO against an application by Excellent First Limited (Cayman Islands) for a new gTLD ".慈善 (Charity)".

13. On 7 May 2013, the Centre informed the Parties that it had decided to consolidate the Objection with the two other above-referenced cases.

14. The Chairman of the Standing Committee having appointed the Expert on 4 July 2013, on 2 August 2013 the Centre confirmed to the Parties the full constitution of the Expert Panel (comprising the Expert as sole member). On the same day, the Centre forwarded the file to the Expert Panel.

15. On 2 August 2013, IO wrote to the Expert Panel requesting leave to file an Additional Written Statement.

16. On 9 August 2013, having considered the Parties' submissions, the Expert Panel wrote to the Parties informing them of its view that it would be assisted by a second round of written submissions and inviting the Parties each to submit an Additional Written Statement in accordance with the following timetable: IO to file its Additional Written

Submission on or before 22 August 2013 and Applicant to file its Additional Written Submission on or before 2 September 2013.

17. On 10 August 2013, IO wrote to the Expert Panel requesting an extension of two days to the timetable for the Additional Written Submissions.

18. On 11 August 2013, Applicant wrote to the Expert Panel stating that it had no objection to IO's requests for a 2 day extension to the timetable.

19. On 13 August 2013, the Expert Panel granted IO's request, extending the deadline for the filing of IO's Additional Written Submission to 24 August 2013 and the deadline for the filing of Applicant's Additional Written Submission to 4 September 2013.

20. On 15 August 2013, the applicant in EXP/395/ICANN/12 requested a further extension of 2 days (i.e., 6 September 2013) for the filing of its additional written statement to which IO indicated on the same day that it had no objection and that such extension would benefit all of the applicants in the consolidated cases, including the Applicant. That extension was therefore extended to Applicant.

21. On 22 August 2013, IO filed by email its Additional Written Statement.

22. On 22 August 2013, the Expert Panel acknowledged receipt of IO's Additional Written Statement and confirmed that the deadline for the filing by Applicant of its Additional Written Submission was 6 September 2013.

23. On 6 September 2013, Applicant filed by email its Additional Written Statement.

24. No hearing took place.

25. The Expert Panel submitted the draft Expert Determination to the Centre for scrutiny under Article 21(b) of the Procedure within the time limit contained in Article 21(a) of the Procedure.

26. In accordance with Article 5(a) of the Procedure, the language of the proceedings is English.

27. In accordance with Article 6(a) of the Procedure, all communications by the Parties with the Centre and the Expert Panel were submitted electronically.

28. Pursuant to Article 4(d) of the Procedure, the place of the proceedings is Paris, France.

4. Issues to be Determined by the Expert Panel

4.1. IO's Impartiality and Independence

4.1.1. IO's Position

29. IO confirms that he is acting exclusively in the best interests of the public who use the global internet and not in accordance with what he himself might prefer or with self-interest[1].

4.1.2. Applicant's Position

30. Applicant does not contest IO's impartiality and independence.

4.2. IO's Standing

4.2.1. IO's Position

31. IO confirms that it meets the standing requirements and other admissibility conditions in section 3.2.5 of the Guidebook.

4.2.2. Applicant's Position

32. Applicant does not contest IO's standing and the admissibility of the Objection.

4.3. The Community Objection

33. IO's objection is a Community Objection to Applicant's Application of ".Charity" as a new gTLD.

[1] IO Additional Written Statement, para. 2.

34. The Expert Panel is therefore to determine whether there is substantial opposition to the Application from a significant portion of the community to which the gTLD string ".Charity" may be explicitly or implicitly targeted (Article 2(e)(iv) of the Procedure).

35. Under section 3.5.4 of Module 3 of the Guidebook, the Expert Panel must be satisfied that IO had proven that (i) the community invoked by IO is a clearly delineated community; (ii) community opposition to the Application is substantial; (iii) there is a strong association between the community invoked and the applied-for gTLD string (".Charity"); and (iv) the Application creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted.

4.3.1. IO's Position

36. According to IO, an objector making a Community Objection must satisfy four tests under section 3.5.4 of the Guidebook. IO states these four tests as: (a) a Community test, namely that the community invoked by the objector is a clearly delineated community; (b) a Substantial opposition test, namely that community opposition to the application is substantial; (c) a Targeting test, namely that there is a strong association between the community invoked and the applied-for gTLD string; and (d) a Detriment test, namely that the application creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted[2].

37. IO argues that the four tests are met. He submits that the applied-for gTLD string ".Charity" targets the charity sector such that the Targeting test is satisfied, even though the Application has not been framed as a community based TLD for the benefit of the charity community[3]. IO states that the charity sector constitutes a clearly delineated community in the sense of the Guidebook, thereby fulfilling the Community test[4]. IO claims that the opposition to the Application is substantial, meaning that the Substantial opposition test is met[5]. Finally, IO pleads that the Application creates a likelihood of material detriment to the rights and legitimate interests of the charity community, fulfilling the Detriment test[6].

[2] Objection, para. 7.

[3] Objection, para 8.

[4] Ibid.

[5] Ibid.

[6] Ibid.

4.3.1.1. *The Community Test*

38. IO's position is that the Community test in the Guidebook does not require that the gTLD string describes a clearly delineated community (which would render the Targeting Test otiose) but that there exists a community identified by the objector comprising a group of persons clearly delineated from others including internet users in general[7].

39. According to IO, the community in question is the charity sector[8], comprising all charitable institutions, including those that are specifically registered or regulated in some form in the states where they operate such that they must be not for profit institutions[9].

40. IO points out that the Guidebook does not provide a clear definition of the term "community". Instead, the Guidebook refers to a non-exhaustive list of factors to which the Expert Panel may refer including the recognition of the community at a local/global level, the level of formal boundaries, the length of existence, the global distribution, or the size of the community[10].

41. For IO, the distinctive element of a community is the commonality of certain characteristics, whatever they might be[11].

42. Referring to Evaluation question No.20 of the Guidebook, Attachment to Module 2, IO argues that a relevant criterion is whether the group of persons comprising the community can be clearly delineated from the others – including internet users in general[12]. Recognition of the community as such (by its members and others) is an important factor in this regard[13].

[7] Objection, para. 16; IO Additional Written Submission, paras 3 to 12.

[8] Objection, para. 19.

[9] Objection, para. 20.

[10] Objection, para. 15 referencing section 3.5.4 of the Guidebook.

[11] Objection, para. 16.

[12] Objection, para. 18.

[13] Ibid.

43. IO points out that charities and charitable organizations (i.e., the charity sector) are included in the "'charity-based enterprises', the providers of 'online charity services' and 'charity information and donation services'" explicitly targeted by the Applicant[14].

44. The common characteristics of the persons comprising the charity sector identified by IO are such persons' "charitable aims", "often the status of a not for profit institution", exemption from a range of regulatory requirements applicable to for-profit entities and funding through donations or public money[15]. Whilst not endorsing Applicant's survey, it notes that 86.6% of the participants associated the term "charity" with donating to a registered organization[16].

45. IO accepts that the charity sector is not an organized community with an entity dedicated to the community and its activities, but argues that the meaning of community in the Guidebook is not limited to organized communities and covers less structured communities, like those based on a common place of origin or a common language or a common activity or common set of goals or interests or values[17] and refers to the 2007 ICANN Final Report which confirms that "community should be interpreted broadly and will include, for example, an economic sector, a cultural community, or a linguistic community"[18].

46. IO points out that the charity sector is delineated as a recognizable community, distinct from others by both its members and the public, referring to public comments made on the meaning of the word "community" in the context of community objections[19]. IO argues that whilst corporations may perform charitable acts, the possibility of competing motives or even ulterior profit making motives sets them apart from the not-for-profit activities of a charity or charitable organization[20].

47. IO underlines that his position is confirmed by the Advice contained in the GAC's Beijing Communiqué dated 11 April 2013[21] which considered the charity community as a market sector delineated by clear and/or regulated entry requirements on account of

[14] Objection, paras 10 & 19.

[15] Objection, para. 20.

[16] IO Additional Written Statement, para. 10.

[17] Objection, para. 21.

[18] Objection, para. 17.

[19] Objection, para. 20 ; IO Additional Written Statement, para. 11.

[20] IO Additional Written Statement, para. 9.

[21] http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf -Annex 1 to IO Additional Written Statement, para. 11.

the level of implied trust from consumers and risk of consumer harm associated with its activities[22]. The GAC included ".Charity" in its list of sensitive strings necessitating safeguard measures[23].

4.3.1.2. The Targeting Test

48. IO argues that the ".Charity" string targets the charity community (comprising charities and charitable organizations)[24] and that therefore the Targeting test is met[25].

49. IO notes that in the Application, Applicant explicitly targets "'charity-based enterprises', the providers of 'online charity services' and 'charity information and donation services'" – which include all charitable institutions[26]. By virtue of Applicant's own statements, therefore, the ".Charity" string explicitly targets the charity sector[27].

50. IO disagrees with Applicant that the word "charity" is a generic term such as the word "book" and argues that the community identified by IO as associated with "charity" is significantly narrower than the stakeholders that might be associated with generic terms such as "book"[28]. IO refers also to one of the meanings of the word "charity" as charities and charitable institutions which indicates that it is generally associated in the public mind with giving for what is seen as a good cause and likewise with not for profit institutions that are directed to some form of charitable outcome[29]. IO adds that simply because the word bears several meanings, this does not preclude the string from having a strong association with one of those meanings if the general public is likely to make that association[30].

51. IO accepts that there may be issues in delimiting the members of the charity sector at the peripheries of the community as a matter of domestic law, but this does not detract

[22] IO Additional Written Statement, para. 11.

[23] Ibid.

[24] Objection, para. 10.

[25] Objection, paras 8 and 14.

[26] Objection, para. 10.

[27] Objection, para. 14.

[28] IO Additional Written Statement, para. 6.

[29] IO Additional Written Statement, para. 5.

[30] Ibid.

from the existence of the charity sector as a community within the meaning of the Guidebook[31].

52. IO concludes that according to Applicant's own statements and the general use of the term "charity" by the public, there is a strong association between the charity sector and ".Charity"[32].

4.3.1.3. The Substantial Opposition Test

53. According to IO, the test whether there is "substantial opposition within the community" to the Application is largely casuistic[33].

54. IO refers to the non-exhaustive list of factors in the Guidebook which an Expert Panel may use to identify substantial opposition to the Application[34] noting that the factors are more useful in cases of well-organized and structured communities than in cases like the present of communities lacking organizational structures or clear representation[35].

55. IO argues that a mere numerical criterion – the number of voiced oppositions to the Application – was not the intent of the Guidebook, the word "substantial" meaning not simply a large number but also something of "considerable importance" or "considerable worth"[36]. IO points out that since a condition for admissibility of an objection by an independent objector is the existence of at least one public comment in opposition, that must mean that an objection can succeed if there is just one such public comment[37]. According to IO, therefore, the material content of comments and oppositions and the rights and interests of those expressing those comments and oppositions must be taken into account[38].

56. IO identifies opposition comments having been posted on the public comments website by the Charity Commission for England and Wales, the National Council for

[31] IO Additional Written Statement, para. 6.

[32] Objection, para. 14.

[33] Objection, para. 22.

[34] Objection, para. 23.

[35] Objection, para. 24.

[36] Objection, para. 25.

[37] IO Additional Written Statement, para. 13.

[38] Objection, para. 25.

Voluntary Organizations and the Association of Charitable Foundations, the first being the regulator of charities in England and Wales and the last representing a membership of some 330 charitable trusts and foundations in England and Wales[39]. IO refers also to the Australian member of the GAC having issued an Early Warning regarding ".Charity"[40]. According to IO, the common underlying concern of such opposition comments and Early Warning is the potential harm to the system of trust on which charities and charitable are largely dependent that would be caused in the absence of sufficient protection mechanisms such as strict eligibility criteria for users of the string[41].

57. IO admits that the opposition to or concerns over the Application have largely emanated from the UK and Australia (respectively) but argues that the concerns that have been voiced are substantively substantial, are "without doubt … of much more general application"[42] and include the views of one or more governments (referencing section 1.1.2.4 of the Guidebook)[43].

58. IO argues that no conclusions can be drawn from non-objections since an independent objector is required to demonstrate substantial opposition from the comments that have been made[44].

4.3.1.4. The Detriment Test

59. IO emphasizes that the Detriment test requires a finding of "a likelihood of detriment"[45] and not of actual detriment – which would be anathema, the string not yet having been put into use[46] – the idea of requiring a finding of actual detriment having been abandoned during the *travaux* of ICANN[47].

[39] Objection, para. 27.

[40] Objection, para. 31.

[41] Objection, paras 27 to 31.

[42] Objection, para. 33.

[43] Objection, para. 32.

[44] IO Additional Written Statement, para. 14.

[45] Objection, para. 34.

[46] IO Additional Written Statement, para. 16.

[47] Ibid.

60. According to IO, the likelihood of detriment must be created by the Application and therefore must take into account the Applicant and the security protection for user and community interests that Applicant has proposed or intends to adopt[48].

61. IO underlines that the likelihood of detriment must be to the rights or legitimate interests of the community or to users more widely, referring to Implementation Guideline P[49]. He refers to the guidance in the Guidebook and summarizes that detriment may include harm to the reputation of the community, interference with the community's core activities, economic or other concrete damage to the community or significant portions of the community[50].

62. IO points out that the Expert Panel may take into account a variety of factors, including the dependence of the community on the DNS for its core activities, the intended use of the gTLD as stated in the Application, the importance of the rights and interests exposed for the community targeted and for the public more generally[51] and whether the Applicant intends to act in accordance with those rights and interests[52].

63. IO argues, in line with the GAC's Beijing Communiqué of 11 April 2013[53], that the charity sector relies on public trust without which its gift and other funding would be threatened. Public regulation exists in many jurisdictions precisely to protect and nurture that trust[54]. Administration of the ".Charity" string outside such or similar protections and safeguards could, according to IO, citing the Charity Commission of England and Wales, lead to "scope for confusion, misunderstanding and, perhaps, deliberate abuse, resulting in turn in significant damage to charities if public support dropped as a result"[55].

64. IO asserts that the Application does not address the specific needs of the charity community and points to four factors that demonstrate a likelihood of detriment to that community: (i) Applicant has not framed the Application as a community based gTLD, thereby avoiding certain consequences for the evaluation of the Application and

[48] Objection, para. 36.

[49] Objection, para. 34.

[50] Objection, para. 35.

[51] Objection para. 35.

[52] Objection, para. 36.

[53] IO Additional Written Statement, para. 24 and Annex 1 thereto.

[54] Objection, paras. 37 & 38.

[55] Objection, para. 39.

the terms (such as user registration requirements) under which the gTLD would be operated[56]; (ii) the manner in which Applicant proposes to address certain of the specific issues of the ".Charity" string is responsive ex-post facto to abuse without requiring stringent registrant eligibility criteria – the needs and requirements of the charity community would not be addressed in a preventive manner with a review after 2 years of operation to monitor abuse and its treatment[57]; (iii) the governance council proposed by Applicant would have a non-binding advisory role which IO considers inadequate protection for the needs (in particular in terms of consumer trust) identified for the charity sector[58]; and (iv) the broad registration criteria proposed by Applicant would enable persons not part of the charity sector (such as commercial bodies) to use the string[59].

65. IO concludes that Applicant fails to address the specific characteristics of the ".Charity" string, including the need to protect public trust in charities and charitable organizations being the community implicitly targeted by the string and instead applies a policy largely identical to that proposed by Applicant's parent and its other subsidiaries for strings with different features such as ".Poker"[60].

4.3.2. *Applicant's Position*

66. Applicant bases its Response on the understanding that an objector making a Community objection must satisfy four tests to succeed, namely, the Community test, the Targeting test, the Substantial Opposition test and the Detriment test[61].

67. Applicant's position is that none of the tests is met by IO[62] and in any event the Objection has become redundant in light of the Eligibility Policy it has submitted to ICANN for inclusion in all registration agreements it enters into with ICANN supported by safeguards ensuring compliance by all registry operators[63].

[56] Objection, para. 42.

[57] Objection, paras 43 & 44.

[58] Objection, para. 45.

[59] Objection, para. 46.

[60] Objection, para. 48.

[61] Response, pages 5 to 15.

[62] Response, page 5.

[63] Applicant Additional Written Statement, page 3.

4.3.2.1. The Community Test

68. Applicant argues that no clearly delineated "charity" community exists for a number of reasons[64].

69. Firstly, Applicant argues that those involved in charity do not necessarily share similar goals, values or interests[65].

70. Secondly, Applicant claims that IO's definition of "community" is different from that of the Guidebook, is more malleable and expansive and being premised on a commonality of characteristics is circular. The commonality of characteristics advocated by IO is superficial and differs based on region[66].

71. Thirdly, Applicant asserts that IO's "charity sector" is an arbitrary subset of the persons targeted by the Application.[67]

72. Fourthly, Applicant points out that there are no or at best a low level of formal boundaries around the "charity community" and considerable uncertainty as to who would be included. IO's idea of delineation from other internet users has no basis in the Guidebook[68].

73. Fifthly, Applicant argues that the "charity community" cannot be measured by time of existence, global distribution or number of members since anyone from the public sector to entrepreneurial philanthropists can engage in charitable activity[69].

74. Sixthly, Applicant points out the word "charity" has many meanings and even within the meaning of "charitable institution" there is considerable difficulty of definition as shown by the history of the Charities Act 2006 in the UK[70]. Further, there is disparity between different countries as to what constitutes a charitable institution – often

[64] Response, pages 5 to 9.

[65] Response, page 5.

[66] Ibid.

[67] Response, pages 5 to 6.

[68] Response, page 6.

[69] Ibid.

[70] Response, page 7.

dictated by political considerations[71]. Within any such definition there is considerable scope for divergent aims and conflicting goals[72].

75. Finally, Applicant asserts that there is a lack of public recognition of the alleged charity community and relies upon its own survey showing that only 5.4% of respondents agreed that only government regulated entities can undertake charitable acts[73].

4.3.2.2. The Substantial Opposition Test

76. Applicant refers to section 3.5.4 of the Guidelines and argues that IO must prove substantial opposition to the Application from the community on whose behalf IO purports to speak[74]. Applicant extracts from that section six factors to be taken into account: (i) the number of expressions of opposition; (ii) the representative nature of those expression opposition; (iii) the stature or weight of the opposition; (iv) the distribution or diversity of opposition within the community; (v) the defence of the community in other contexts by those expressing opposition; and (vi) costs incurred in expressing opposition[75].

77. Applicant points out that the dozen or so public commentators, which are mainly sourced from the UK, are far outnumbered by the large non-objection populations of the "charity" community (including worldwide charitable organizations, corporate and entrepreneurial philanthropists, charity services and individuals engaging in charitable acts). Although for Applicant the content of comments is irrelevant for assessing whether there is "substantial" opposition, Applicant notes that several have identical wording and originated from a single source following an orchestrated campaign against the applications for ".Charity"[76].

78. Applicant disputes the representative nature of the opposition comments – constituting at best 1% of the global population and the absence of any comments from

[71] Ibid.

[72] Response, pages 7 to 9.

[73] Response, page 9.

[74] Ibid.

[75] Response, pages 9 to 10.

[76] Response, page 9.

unregistered charities, corporate and entrepreneurial philanthropists, charity services and individuals engaged in charitable acts[77].

79. Applicant states that the relative stature and weight of the opposition comments is limited given the many important non-objecting stakeholders[78]. Applicant asserts that the Australian GAC member Early Warning is not evidence of substantial opposition (given the purpose of GAC early warnings) and in any event misrepresents the situation of charitable organizations worldwide (assimilating them to those regulated in the UK or Australia)[79].

80. Applicant asserts that the diversity of the opposition comments is minimal relative to the non-objecting stakeholders[80].

81. Applicant points out that no evidence has been adduced by IO as to the costs incurred by those expressing opposition[81].

4.3.2.3. The Targeting Test

82. Applicant relies on section 3.5.4 of the Guidebook and argues that IO must prove a "strong association" between the applied-for string and the community he invokes by relying on statements in the Application, public statements by the Applicant and public associations between the string and the community[82].

83. Applicant criticizes IO for having relied upon a derivative association between the applied-for string and the "community sector" arguing that the string is more strongly associated with the broader group actually targeted by Applicant[83].

84. Applicant argues that there is at best an ancillary or derivative public association of the ".Charity" string with the "charity sector" – relying on its survey[84].

[77] Response, page 10.

[78] Ibid.

[79] Ibid.

[80] Ibid.

[81] Ibid.

[82] Response, page 11.

[83] Ibid.

[84] Ibid.

4.3.2.4. Detriment Test

85. According to Applicant who relies on section 3.5.4 of the Guidebook, the detriment test requires an independent objector to prove "likelihood" of "material detriment" which in turn calls for proof of (i) the nature and extent of potential damage to the "community" or its reputation from Applicant's operation of the string; (ii) evidence that Applicant does not intend to act consistently with the interests of that "community"; (iii) interference with the core activities of that "community" by Applicant's operation of the string; (iv) the extent to which the "community" depends on the DNS for core activities; and (v) the level of certainty that detrimental outcomes will occur[85].

86. Applicant criticizes IO for limiting its arguments to the attraction of gifts of money and time and services from donors, the definition of charity being much broader[86]. Applicant underlines its sensitivity to the concerns expressed by IO and argues that the robust policies and mechanisms that it is offering address those concerns with the Governance Council it is proposing being a platform for the charity sector to shape the policies of the gTLD's operation, consumer trust being a core operating and abuse detection and sanctioning principle, and registry surveys ensuring monitoring of those policies and principles[87]. Applicant disagrees with IO's strict registration criteria arguing that they would not be possible on a global level given the diversity of meanings of "charity"[88].

87. Applicant argues that many of the public comments are not representative of the interests of the group targeted by the Application, that the Governance Council will be a platform for those interests to shape operating policies, and that the Applicant undertakes to try in good faith to operate the gTLD in an inclusive and respectful manner as evidenced by the mechanisms it will apply[89].

88. Applicant asserts that there is no evidence that the core activities of the alleged charity sector will be interfered with. On the contrary, Applicant argues that the mechanisms it will introduce will protect those core activities (including through the Governance

[85] Response, pages 11 to 15.

[86] Response, page 11.

[87] Response, pages 11 to 12.

[88] Response, page 12.

[89] Response, pages 12 to 13.

Council)[90]. For Applicant, the fact that it has not made a community-based application for the gTLD is a factor of the lack of clear delineation of the supposed community[91]. Applicant points out that the core activities of the "charity" community are independent of the gTLD and will be enhanced by the string[92].

89. Applicant points out that there is no evidence of the alleged "charity" community being dependent upon the DNS – with much charitable giving taking place off-line[93].

90. In its Additional Written Statement, Applicant argues that the Objection has become redundant on account of the eligibility policy that it has submitted to ICANN as an amendment to its Public Interest Comment Specification which will be included in any registry agreement which Applicant would sign with ICANN if its Application is successful and which Applicant will therefore be contractually obliged to implement at the risk of legal action under the PIC Dispute Resolution Procedure in the event of breach. Applicant states that its eligibility policy defines a "subset of the community" targeted by the applied-for string[94]. Registration will be limited to that subset[95]. The policy limits eligibility to "incorporated entities, unincorporated associations or entities, foundations or trusts which can establish that they are a charity or 'not for profit' enterprise with charitable purposes"[96]. Each registrant applicant must provide the registrar with evidence that either (i) it is a charity or equivalent with a governmental body (other than a tax authority) or organization authorized by a government body to maintain such registration; or (ii) if exempt from such registration requirements on grounds of size, evidence that it would not be required for such registration on the basis of such exemption; or (iii) it is registered with a tax authority as a charity or not for profit organization and evidence of activities restricted to "charitable purposes for the public benefit" within the meaning of the UK Charities Act 2011 (or any replacement legislation) or broadly equivalent activities considered charitable and eligible for tax advantages in its jurisdiction of domicile or incorporation; or (iv) evidence that it is a not for profit organization prohibited from making distributions to members and evidence of activities restricted to "charitable purposes for the public benefit" within the meaning of the UK Charities Act 2011 (or

[90] Response, pages 12 to 13.

[91] Response, pages 13 to 14.

[92] Response ,page 14.

[93] Ibid.

[94] Applicant Additional Written Statement, pages 3 to 4.

[95] Applicant Additional Written Statement, page 3.

[96] Annex 2 to Applicant Additional Written Statement.

any replacement legislation) or broadly equivalent activities considered charitable in its jurisdiction of domicile or incorporation[97]. Acceptable evidence includes, but is not limited to organization documents, statutory restrictions, binding agreements or commitments enforceable by third parties. Subsequent failure to meet an applicable eligibility requirement allows the registry to cancel the registration[98]. Various safeguards are promised with respect to registry operators to ensure compliance with the foregoing[99].

91. Applicant states that the eligibility policy has been developed following and in response to charity sector, its own research on charity regimes around the world and in view of the Objection[100]. Applicant points out that it has defined the policy in part based on UK law which has one of the most developed charities law regimes in the world[101].

5. EXPERT PANEL'S DETERMINATION

5.1. IO's Independence and Impartiality

92. There being no challenge to IO's independence and impartiality, the Expert Panel accepts IO's confirmation of the same.

5.2. IO's Standing

93. As an independent objector, IO fulfills the standing requirement of the Guidebook to make a Community Objection. There being no challenge to the existence of the admissibility conditions, the Expert Panel determines, therefore, that this Objection is admissible.

[97] Ibid.

[98] Ibid.

[99] Ibid.

[100] Applicant Additional Written Statement, page 3.

[101] Ibid.

5.3. The Community Objection

94. In order for his Objection to succeed under section 3.5.4 of the Guidebook, IO bears the burden of proving that four tests are met: (a) a Community test, namely that the community invoked by the objector is a clearly delineated community; (b) a Substantial Opposition test, namely that community opposition to the application is substantial; (c) a Targeting test, namely that there is a strong association between the community invoked and the applied-for gTLD string; and (d) a Detriment test, namely that the application creates a likelihood of material detriment to the rights or legitimate interests of a significant of the community to which the string may be explicitly or implicitly targeted.

5.3.1. The Community Test

95. Pursuant to section 3.5.4 of the Guidebook, IO has the burden of proving to the Expert Panel that *"the community invoked by the objector is a clearly delineated community"*.

96. The "community" in question is the one invoked by the objector – it is not the community targeted by the string, the applicant or the application.

97. The objector in this case is IO. The community invoked by IO is "the charity sector" comprising all "charitable institutions".

98. The question for determination, therefore, is whether IO has proven to the Expert Panel that the "charity sector" comprising all "charitable institutions" constitutes a "clearly delineated community".

99. The Guidebook does not provide a definition of "clearly delineated community" but lists five factors that an Expert Panel may balance when making its determination. That list is neither exhaustive, conclusive nor imperative. None of the cited factors goes to the heart of what is a "community" but each assists in identifying a "community" when it exists: public recognition of the community, level of formal boundaries, length of existence, global distribution and number of members.

100. IO and Applicant agree that for a community to exist there must be a degree of "communality" among the members whether of "interest" or "characteristics" but disagree over the degree of commonality required. The Expert Panel is not convinced by Applicant's arguments that among charitable institutions around the world the

various interests and characteristics are diverse and sometimes conflicting such that the "charity sector" is in fact an arbitrary delineation. Whilst the aims of charitable activities can be widely different and conflicting it is the functioning characteristics of charities and charitable institutions which set them apart from others: status as not-for-profit institutions, often exemption from regulatory requirements applicable to for-profit entities and funding through donations or public money. Given the obviousness of each of these characteristics in the Expert Panel's view, none requires the support of specific evidence to be found as facts. Indeed, the very fact that Applicant has defined its eligibility policy around the "charity sector" based upon the meaning of that community in UK legislation suggests that the community is capable of clear delineation.

101. Indeed, the existence in many jurisdictions, such as the UK, of regulators of the charity sector is an indication that that sector is capable of delineation and is considered publicly to be different from others. The Expert Panel acknowledges differences in definition of charitable institutions and their regulation around the world which leads to a problem of boundary definition and ascertainment of global distribution. However, it is of the view that such differences are at the periphery of the community definition which is not a conclusive factor. ICANN recognizes (for instance in its Final Report of 2007) that precise definition of communities is unnecessary.

102. The public comments made with respect to the Application indicate that publicly the charity sector is considered to exist separately from other sectors of activity. The survey submitted by Applicant lacks acceptable representative criteria and is capable of a multitude of different analyses, but the Expert Panel notes that there is considerable recognition among respondents that "charity" is associated with giving to a registered organizations – one of the key characteristics of the charity sector as defined by IO.

103. IO accepts that the "charity sector" has no clear geographical boundaries – indeed it is global – and is not structured in any way. These are factors which may be taken into account as indices of the absence of a community but are not conclusive.

104. Balancing these various factors and considerations, the Expert Panel finds that the charity sector, comprising all charitable institutions, constitutes a clearly delineated community within the meaning of section 3.5.4 of the Guidebook. The "Community test" has therefore been passed by IO.

5.3.2. *The Targeting Test*

105. Pursuant to section 3.5.4 of the Guidebook, IO has the burden of proving *"a strong association between the applied-for gTLD string and the community"* invoked by the objector.

106. The "strong association" sometimes referred to as "targeting", that must be shown by IO to exist therefore is between the applied-for gTLD and the community invoked by IO: namely, between ".Charity" and the "charity sector".

107. The Guidebook does not define "a strong association" or "targeting" but identifies three sources of evidence that an independent objector may use to show that it exists: statements in the application, other public statements by the applicant and associations by the public. Those three factors are neither exhaustive, imperative nor conclusive.

108. In the Application, Applicant states that the applied-for gTLD is aimed at "charity-based enterprises", "the providers of online charity services" and "charity information and donation services". Following the introduction of its eligibility policy, however, the targeting of the ".Charity" gTLD of the Application corresponds to the community identified by IO.

109. That targeting is supported by Applicant's own survey (despite its failings) which shows that a high percentage of respondents understand the word charity to refer to giving to a registered organization, thus singling out that specific meaning of the word "charity" from others.

110. The GAC Beijing Advice provides further evidence that the public would associate ".Charity" with charitable institutions – the charity sector – given the concern expressed over the sensitive nature of the applied-for gTLD string precisely because of the regulated nature of the charity sector and level of implied trust from consumers invoked by the string. Such concern implies the "strong association" required by the Targeting test.

111. The Expert Panel is therefore satisfied that IO has proven that the requirements of the Targeting test are met.

5.3.3. *The Substantial Opposition Test*

112. Substantial opposition is not defined in the Guidebook other than to indicate that the opposition is to be to the application (as opposed to the Applicant). Instead, section

3.5.4 of the Guidebook provides a list of factors which the Expert Panel may balance to determine whether substantial opposition to the Application exists. That list is neither exhaustive, imperative nor conclusive.

113. IO and Applicant disagree over the meaning of "substantial". IO argues that "substantial" may refer to the number of statements of opposition relative to the composition of the community and/or to the substantive importance or worth of the statements of opposition. Applicant considers that the factors listed in section 3.5.4 of the Guidebook should be applied in accordance with their terms which exclude the substantive subjective importance of any given view the latter being relevant to the Detriment test only.

114. A review of the factors listed in section 3.5.4 indicates that a mere numerical meaning for "substantial" would be wrong. Those factors include not only the relative number of statements of opposition but also the representative nature of those expressing opposition and the recognized weight or stature of the expressions of opposition.

115. IO relies upon public comments from the Charity Commission for England and Wales, the National Council for Voluntary Organizations, the Association of Charitable Foundations, the Australian member of the GAC (in the form of an Early Warning) and the Office of the Scottish Charitable Regulator (as part of a legal rights objection). The Charity Commission is the regulator of charities in England and Wales. The Association of Charitable Foundations represents some 330 charitable trusts and foundations in England and Wales. The National Council for Voluntary Organizations represents just under 10,000 voluntary organizations (not all charitable institutions) in the UK. The Office of the Scottish Charitable Regulator is the regulator of charities in Scotland. The Australian member of the GAC is a representative of the Australian government.

116. The Charity Commission for England and Wales, the Office of the Scottish Charitable Regulator, the Association of Charitable Foundations and the National Council for Voluntary Organizations state their opposition on the basis of the potential harm to the system of trust on which charities and charitable giving are dependent if the ".Charity" string were to be run by a for-profit organization – arguing that had the Application been made as a community-based application their concerns would be assuaged given the status requirements for a community-based applicant. Similar concerns are expressed by the Australian member of the GAC.

117. IO refers to the other public opposition comments made to ICANN[102]. These include opposition from the ACC which has over 30,000 members (in-house counsel) employed by over 10,000 organizations in more than 75 countries. The Association's Not-for-profit Organizations Committee offers a collective voice to over 1,400 in-house counsel practising law in nonprofit institutions across the globe. In addition to concerns over abuse (for which the ACC proposes two types of safeguards), the ACC points to the need for protection *"given the intimate and obvious connection between [.Charity] and our members' organizations that operate in the philanthropy field"*.

118. Applicant's focus on non-objecting stakeholders is unhelpful and not referenced in the Guidebook. Indeed, without evidence as to why stakeholders have not filed objections no helpful conclusions can be drawn.

119. The relative number of statements of opposition is small. Those statements come from the same or similar common law jurisdictions. These are two factors that militate against a finding that there is substantial opposition.

120. This small number of opposition statements comes from bodies that are representative of a larger number of members of the charity sector not only in jurisdictions where regulation of charitable activities is historically strong, developed and well-established but also in the case of ACC, worldwide. These are factors which militate in favour of a finding that there is substantial opposition.

121. The fact that the opposition raised by the different statements is substantively similar does not detract from the number of statements or from their representative nature or relative importance.

122. On balance, the Expert Panel is satisfied that IO has provided evidence of substantial opposition to the Application such that the Substantial opposition test has been passed.

5.3.4. The Detriment Test

123. Pursuant to section 3.5.4 of the Guidebook it is for IO to prove that the Application (or rather use of the applied-for gTLD as contemplated by the Application) creates a likelihood of material detriment to the rights or legitimate interests of a significant portion of the community to which the string may be explicitly or implicitly targeted.

[102] http://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments

124. The test requires evidence of a likelihood of material detriment and not evidence of actual detriment – which would be impossible given the prospective nature of the objection process.

125. Evidence of a likelihood of something happening – cause and effect occurring in the future – is inherently difficult. It is no doubt for this reason that the Guidebook focuses on a variety of factors (none of which is imperative or conclusive) that IO may prove to lead to the conclusion that material detriment is likely. These factors include the dependence of the community on the DNS for its core activities, the intended use of the gTLD as stated in the Application, the importance of the rights and interests exposed for the community and the public, and whether the Applicant intends acting in accordance with those rights and interests.

126. The various public statements of opposition to the Application are all premised on the importance of the global internet as a means of recognition and fund-raising for the charity sector. It is therefore generally accepted that the DNS is important for a core activity of the community.

127. Those public statements of opposition all focus on the need clearly to distinguish charitable organizations from for-profit enterprises in particular in public giving and fund-raising activities. They point out the absence, prior to the introduction by Applicant of its eligibility policy, of any limitation in the Application of the ".Charity" string to not-for-profit or charitable organizations. This concern is the origin of the suggestion in many of the public statements of opposition that the ".Charity" string should be treated only as a community-based gTLD.

128. The public statements of opposition identify the rights and interests of the community and the public that are exposed to harm if the Application were to proceed as the need of the charity sector for public funding to finance its activities; the trust and confidence of the public in the charity sector that donations will be used for the stated charitable ends. They point out that those rights and interests are protected outside the internet by public regulation of recourse to public giving for charitable purposes. They, and IO, emphasize the need for strict registration eligibility criteria limited to persons regulated as charitable bodies or their equivalent depending upon domestic law.

129. The eligibility policy defined by Applicant and inspired by the criteria of the UK Charities Act 2011 which will be included in any registration agreement entered into by Applicant with ICANN together with appropriate safeguards for registry operators respond in the Expert Panel's view to the Detriment test concerns raised by IO.

130. In particular the defined "subset of the community" to which registration will be limited consists of "incorporated entities, unincorporated associations or entities, foundations or trusts which can establish that they are a charity or 'not for profit' enterprise with charitable purposes"[103]. The process for registration will require each registrant applicant to provide the registrar with evidence that either (i) it is a charity or equivalent with a governmental body (other than a tax authority) or organization authorized by a government body to maintain such registration; or (ii) if exempt from such registration requirements on grounds of size, evidence that it would not be required for such registration on the basis of such exemption; or (iii) it is registered with a tax authority as a charity or not for profit organization and evidence of activities restricted to "charitable purposes for the public benefit" within the meaning of the UK Charities Act 2011 (or any replacement legislation) or broadly equivalent activities considered charitable and eligible for tax advantages in its jurisdiction of domicile or incorporation; or (iv) evidence that it is a not for profit organization prohibited from making distributions to members and evidence of activities restricted to "charitable purposes for the public benefit" within the meaning of the UK Charities Act 2011 (or any replacement legislation) or broadly equivalent activities considered charitable in its jurisdiction of domicile or incorporation[104]. Acceptable evidence includes, but is not limited to, organization documents, statutory restrictions, binding agreements or commitments enforceable by third parties. Subsequent failure to meet an applicable eligibility requirement will allow the registry to cancel the registration[105]. Various safeguards are promised with respect to registry operators to ensure compliance with the foregoing[106]. In short, registration will be limited to members of the charity sector as narrowly defined by analogy with the definitions of "charity" and "charitable purposes for the public benefit" found in the UK Charities Act 2011.

131. According to Applicant, the eligibility policy has been developed following and in response to charity sector comments, its own research on charity regimes around the world and in view of the Objection[107]. Applicant points out that it has defined the policy in part based on UK law which has one of the most developed charities law regimes in the world[108].

[103] Annex 2 to Applicant's Additional Written Statement.

[104] Ibid.

[105] Ibid.

[106] Ibid.

[107] Applicant Additional Written Statement, page 3.

[108] Ibid.

132. Provided that Applicant's undertaking is honoured, the Expert Panel considers, therefore, that there would be no material detriment as identified by IO to the charity sector – registrants being limited to the members of that sector.

133. In view of the foregoing, the Expert Panel finds that IO has failed to prove that the Detriment test has been met.

5.3.5. Conclusion

134. Having reviewed the Parties' submissions and supporting evidence and for the foregoing reasons, one of the four tests not having been proven, the Expert Panel rejects IO's Community objection against the Application.

5.4. Costs of the Expert Determination

135. Article 14(e) of the Procedure provides which of the Parties shall bear the Costs.

136. The Objection has been rejected.

137. In accordance with Article 14(e) of the Procedure, the advance payment on Costs made by Applicant is therefore to be reimbursed to it.

5.5. Expert Panel's Determination

138. In the light of the above and in accordance with Article 21(d) of the Procedure, I hereby render the following Expert Determination:

i. The Independent Objector's Objection is rejected and Applicant Spring Registry Limited prevails.

ii. The advance payment of Costs made by Applicant shall be reimbursed to it by the Centre pursuant to Article 14(e) of the Procedure.

Done in Paris

9 January 2014

Mr. Tim Portwood
Expert Panel

Attachment 10

[SRL 25 Oct. 2013 supplemental filing and linked evidence]

RE: EXP/400/ICANN/17 Rejoinder

Peter Young <pyoung@famousfourmedia.com>

Fri 10/25/2013 5:24 AM

To Contact Information Redacted

Contact Information Redacted

Cc

Dear Mr Portwood

I refer to our Rejoinder of 6th September.

I apologise for the unsolicited communication, but, since filing of our earlier Rejoinder, our amended PIC SPEC referred to therein has been published by ICANN for public comment:

https://gtldresult.icann.org/application-result/applicationstatus/applicationchangehistory/1186

I make this submission merely to make you aware of independent evidence that our eligibility policy is progressing through the new gTLD application process, and in the interests of justice I hope you can consider this evidence. It merely confirms what was stated in our Rejoinder, and should only take a moment to consider.

Articles 17 and 18 of the Dispute Rules do provide the Panel with the power to admit additional material, and making this submission is the only way to draw it to your attention.

Yours sincerely

Peter Young

Peter Young
Managing Director/Chief Legal Officer
Famous Four Media Limited
Contact Information Redacted

From: Peter Young
Sent: 06 September 2013 11:44
To: Contact Information Redacted
Cc: Contact Information Redacted
Contact Information Redacted
Contact Information Redacted
Subject: RE: EXP/400/ICANN/17 Rejoinder

Dear Mr Portwood

I attach our written rejoinder and supporting annexes for your kind consideration.

Kind regards

Peter Young
For and on behalf of Spring Registry Limited

From: Alain Pellet Contact Information Redacted
Sent: 22 August 2013 20:11
To: Contact Information Redacted
Cc: Contact Information Redacted
Contact Information Redacted
Con ac nforma ion Redac ed ICC; Wordsworth, Sam; Van Den Biesen, Phon; "Müller , Daniel"; "Bajer Pellet, Héloïse"
Subject: EXP/400/ICANN/17 Additional Written Statement

Dear Mr. Portwood,

By e-mail of 2 August 2013, I requested authorization to file an additional written statement in order to address new issues which have been raised by the Applicant's response. This request was granted and I thank you sincerely for this opportunity.

Accordingly, please find attached the above mentioned additional written statement, as well as its annex, regarding my Community objection against the gTLD string .Charity applied-by Spring Registry Limited, case EXP/400/ICANN/17.

I remain at your disposal should you need any further information.

Sincerely,

Alain PELLET
ICANN - Independent Objector

gTLD String: .charity
Applicant Entity Name: Spring Registry Limited
Application ID#: 1-1241-87032

SPECIFICATION 11
PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on 27 June 2013in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. Registry Operator will operate the registry for the TLD in compliance with all commitments, statements of intent and business plans stated in the following sections of Registry Operator's application to ICANN for the TLD, which commitments, statements of intent and business plans are hereby incorporated by reference into this Agreement. Registry Operator's obligations pursuant to this paragraph shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN ((posted at [url to be inserted when final procedure is adopted]), which may be revised in immaterial respects by ICANN from time to time, (the "PICDRP"). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

The Registry Operator appreciates the opportunity to restate and once again commit to the following operational measures, where those matters are within its control, as outlined in our application. We reserve the right to amend or change this PIC Spec once the details of the Program are finalized.

In addition to the ICANN mandated minimum mechanisms, the Registry Operator will deploy the following to prevent and mitigate domain name abuse and aid in rights protection:

Abuse Prevention and Mitigation plan: The Registry Operator will be implementing a thorough and extensive Abuse Prevention and Mitigation plan as outlined in our response to Question 28. The APM plan is designed to minimise abusive registrations and other detrimental activities that may negatively impact internet users. This plan includes the establishment of 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 gTLD through all Registrars of record, including those involving a reseller.

Additional Mechanism for Protection of Capital City Names: The Registry Operator will implement an additional mechanism for protection of Capital City Names as outlined in section 6.1 of our response to Question 28. The Capital City Claim will grant additional protection to the capital city names of a country or territory listed in the ISO 3166-1 standard.

Additional Mechanisms to Protect and Reserve IGO Names: The Registry Operator will implement Additional Mechanisms to Protect and Reserve IGO Names as outlined in section 6.2 of our response to Question 28. The Registry Operator considers the Protection of Intergovernmental Organization (″IGO″) names to be very important. The Registry Operator will use strings registered as second level domains in the .int gTLD as the basis for this protection but the Registry Operator has committed to working with the GAC to protect a future list of IGO names which the GAC may prepare.

Additional Mechanism - Abuse Prevention and Mitigation Seal: The applicant intends to further augment the security and stability of its gTLD by implementing the Abuse Prevention and Mitigation Seal (the "APM Seal") as outlined in section 6.3 of our response to Question 28. The APM Seal will provide users and stakeholders in the sector with a one-click mechanism for how to access relevant Abuse

Prevention and Mitigation processes and will include an ip address geo-location mechanism that will provide enhanced features for website visitors from specific geographic regions. Registrants on the gTLD will be required to implement an APM Seal on their web pages that users can click-on and be taken to a web resource detailing the relevant mechanisms for how to report and address abuse on the gTLD.

Acceptable Use Policy: The Registry Operator will develop an Acceptable Use Policy as described in section 14 of our response to Question 28. This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its Registrar partners and/or that may put the safety and security of any Registrant or user at risk. The process also allows the Registry to take preventive measures to avoid any such criminal or security threats.

Right Protection Mechanisms: The Registry Operator is firmly committed to the protection of Intellectual Property rights and to implementing the mandatory RPMs contained in the Registry Operator Guidebook and detailed in Specification 7 of the Registry Agreement. Use of domain names that infringe upon the legal rights of others in the gTLD will not be tolerated and preventing abusive registrations is a core objective of the Registry Operator.

WHOIS Accuracy: The Registry Operator will undertake efforts to promote WHOIS Accuracy as outlined in section 5 of our response to Question 29. This will include searchable WHOIS and Audits.

The Registry Operator is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the AUP are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or are part of a real-time investigation by law enforcement. Certain of the above commitments referenced in Question 28 and 29 will require the cooperation of the Registrar channel and the Registry Operator commits to using commercially reasonable efforts to ensure such cooperation.

Our discussions with various governments to resolve early warnings continue and we reserve right to amend or change this PIC Spec once these discussions successfully conclude.

3. Registry Operator agrees to perform following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets.

Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

c. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies.

d. Registry Operator of a “Generic String” TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person’s or entity’s “Affiliates” (as defined in Section 2.9(c) of the Registry Agreement). “Generic String” means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others.

Further, Registry Operator commits to establishing and enforcing registration eligibility policies, and to implementing the APM seal on a geo location basis to enable enforcement, with respect to the .CHARITY TLD as follows:

Eligibility Policy

Only incorporated entities, unincorporated associations or entities, foundations or trusts which can establish that they are a charity or “not for profit” enterprise with charitable purposes will qualify to be a registrant of a .CHARITY domain name.

As part of the registration process for the .CHARITY TLD, potential applicants must provide the registrar with the following evidence and criteria, which will be applied to determine eligibility:

- Registration as a charity or equivalent with a governmental body (other than a tax authority) or an organisation authorised by a governmental body to maintain such registrations; or

- If exempt from registration requirements on the grounds of size, evidence acceptable to the Registry that it would be required to be registered as per the above but for such exemption; or

- Registration with a tax authority, as a charity or not for profit organisation **combined with** evidence acceptable to the Registry of activities restricted to “charitable purposes for the public benefit” as set out in Charities Act 2011 (or any replacement legislation) of the United Kingdom or broadly equivalent activities which are considered charitable and hence eligible for tax advantages in its jurisdiction of domicile or incorporation; or

- Evidence acceptable to the Registry that the organisation is not for profit in that the organisation cannot make distributions to members **combined with** evidence acceptable to the Registry of activities restricted to “charitable purposes for the public benefit” as set out in Charities Act 2011 (or any replacement legislation) of the United Kingdom or broadly equivalent activities which are considered charitable in its jurisdiction of domicile or incorporation.

- "Evidence acceptable to the Registry" would include (but is not limited to) organisational documents, statutory restrictions, binding agreements, binding resolutions or commitments enforceable by third parties.

If at any time during the term of registration of a Registered Name a registrant shall no longer meet the requirements of the Eligibility Policy, then, in addition to any other rights of the Registry existing under the RRA between the Registry and any applicable registrar or otherwise, the Registry reserves the right to deny or cancel the registration, renewal, or transfer of any Registered Name, or to place any Registered Name on registry lock, hold, or similar status, with respect to any such Registered Name that the Registry, upon reasonable belief formed after reasonable investigation, deems to be registered to a registrant that is not in compliance with the Eligibility Policy.

Enforcement and the APM Seal

The .CHARITY TLD will benefit from the implementation of the APM seal as described in the application. This will facilitate reporting of breaches of and enforcement of the Eligibility Policy, a breach of which will also be reportable and actionable by the Registry in the same manner as a breach of the Acceptable Use Policy. We hereby clarify that the technical implementation of the APM Seal program as described in the application includes the following functionality:

1) Countries may designate, through participation in the Governance Council, which APM Seal TLD Registries they are interested in and participate in the program directly with the registry. Each country will have the opportunity to develop an information page specific to each TLD they are interested in.

2) Using geo location ip address technology, when a visitor from a country who is participating in the APM Seal Program visits a website in the APM Seal TLD program, a notice will be displayed to the visitor. By clicking on the Seal, users will then be taken to the country specific information page developed by each country for their citizens.

3) The Advanced APM seal will only be displayed to visitors from countries which have chosen to participate in the Advanced APM Seal program.

4) As these TLDs mature and to allow for updated regulatory or legislative developments, Country Specific Advanced APM Seal information pages can be updated as necessary.

Attachment 11

[SRL Application No. 1-1241-87032 for <.CHARITY>]

New gTLD Application Submitted to ICANN by: Spring Registry Limited

String: charity

Originally Posted: 13 June 2012

Application ID: 1-1241-87032

Applicant Information

1. Full legal name

Spring Registry Limited

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Mr. Geir Andreas Rasmussen

6(b). Title

Chief Executive Officer - Famous Four Media Limited

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

+350 200 510 71

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Brian Winterfeldt

7(b). Title

Partner - Steptoe & Johnson LLP

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

+12022617547

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited Liability Company

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Incorporated under the Gibraltar Companies Act 1930

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

Domain Venture Partners PCC Limited

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Domain Management Limited	Director

11(b). Name(s) and position(s) of all officers and partners

Charles Ashley Richard Melvin	Chief Operating Officer
Iain Simon Roache	Chief Executive Officer
Timothy James Ireton	Chief Financial Officer

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

Domain Venture Partners PCC Limited	Not applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

```
charity
```

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. 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.

Q16
The Applicant has taken steps to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string (the “String”). The following has been undertaken:

a)The TLD label is valid as specified in relevant technical standards, including: Domain Names: Implementation and Specification (RFC 1035), and Clarifications to the DNS Specification (RFC 2181) and any updates thereto;

b)The TLD label, which is 7 characters long, is well short of the 63 character maximum length;

c) The TLD label is a valid host name, as specified IN: DOD Internet Host Table Specification (RFC 952), Requirements for Internet Hosts — Application and Support (RFC1123), and Application Techniques for Checking and Transformation of Names (RFC 3696), Internationalized Domain Names in Applications (IDNA)(RFCs 5890-5894), and any updates thereto;

d)The TLD label consists entirely of letters (a-z)

The Applicant has evaluated the risks of the TLD experiencing TLD Acceptance issues similar to problems reported in the “Evaluation of the New gTLDs: Policy and Legal Issues” (31⁄08⁄2004) which discussed acceptance issues associated with the year 2000 round of new gTLDs with more than three characters (i.e.,.aero,.coop,.info, .museum, .name). At that time, only one gTLD, .arpa, which is not widely used outside of limited circles - had four letters. As a result, the new gTLDs had compatibility problems with the software used by Internet infrastructure operators and application providers. Some users have recently been reporting issues with the use of .xxx names in applications such as Twitter and Skype where domain names entered from that TLD are not instantly recognized with a hyperlink as more established gTLDs are.

The Applicant’s registry backend services provider, Neustar Inc tested the String for potential rendering or operational problems; none were found.

As the String is not an IDN it does not contain characters that require mixed right-to-left or left-to-right functions. The applicant has familiarized itself with the requirements and components of the IDNA protocol by reviewing the RFCs and background information found on the ICANN IDN Wiki.

The Applicant tested the String using the ICANN SWORD String Similarity Assessment Tool algorithm. The result of this test is 53. The Applicant considers this to be below the level where issues might occur. Should Registrants experience any acceptance issues the Applicant will have a dedicated Operational and Rendering Team (“ORT”) on an on-going basis to assist with operational, rendering issues or any other problems that might arise. The ORT will be in place to assist Registrants with any additional problems that may arise out of new TLD that other applicants may be awarded during this process which could lead to unforeseen string confusion now and in the future.
-end-

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

Q18A
Mission and Purpose of .charity?
The Applicant’s mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. Its aim is to become the premier online destination for such creators and their wide range of users. The Applicant will create an Internet space whose central function is to provide a platform for creating, producing and disseminating informative, creative and innovative content that is easily recognizable as pertaining to its stakeholder group. The Applicant is acutely aware of the importance of ICANN’s mission in coordinating the global Internet’s systems of unique identifiers and ensuring their secure and stable operation. The Applicant’s core focus is to create a secure, sustainable, and specialized gTLD, thus supporting ICANN’s primary goals for this program in promoting consumer trust, consumer choice, competition and innovation.

Why .charity?
Charitable giving and deeds endorse and reinforce perhaps some of the most admirable human qualities. Giving to those less fortunate is a notion which pervades moral codes across religions and societies throughout the world. The dawn and development of the internet has brought with it the possibility of learning about misfortunes and injustices across the world and provided many with the potential of acting on their

humanitarian instincts where otherwise they could not have.

However, access to the countless benefits and opportunities which the internet offers can often be hindered when navigating the ever-expanding sea of irrelevant and sometimes malicious content which also exists, and this is as true of online charitable services as anything else.

Thus, the aim of '.charity' is to create a blank canvas for online charity services set within a secure environment. The Applicant will achieve this by creating a consolidated, versatile and dedicated space to access charity information and donation services. As the new space is dedicated to those within this affinity group the Applicant will ensure that consumer trust is promoted. Consequently consumer choice will be augmented as there will be a ready marketplace specifically for charity-based enterprises to provide their goods and services. All stakeholders within the sector will be able to sample reactions to new ideas, or gather thoughts on the improvements of established ones. This will drive innovation and competition, as new channels will be available which are not yet fulfilled by current market offerings, compelling registrants to seek new and varied ways to separate themselves from the competition.

How will .charity take shape?
The Applicant believes that the success of the gTLD will be determined largely by the sector's key global stakeholders. These stakeholders will be interested in registering a domain and additionally be motivated to protect their sector from detrimental practices. The Applicant believes that stakeholders should have the opportunity to influence the gTLD and the way it is governed. Accordingly, the Applicant is establishing a Governance Council ("GC"), consisting of key stakeholders that will serve as an advisory body.

Why Applicant?
The Applicant has substantial combined experience amongst its team in managing global businesses from a financial, legal and operational perspective and an exceptionally strong financial position. The Applicant's Team has previous experience with the entire gTLD life-cycle significantly lowering any launch and ongoing operational risks associated with this application. The Applicant has engaged a world-class Registry services provider to manage the technical infrastructure of the .charity gTLD. The Applicant is further advised by the leading sector experts in all other areas required to ensure a responsible and successful launch and ongoing management of the gTLD to the benefit of all stakeholders in the ICANN community.

Information for future studies and reviews
The Applicant recognizes the connection of the new gTLD application to the Affirmation of Commitments ("AoC"). To gauge the success of the new gTLD program, the Applicant recognizes that an AoC Review Team will be formed one year after the first delegation. To prepare for this, the ICANN Board resolved the creation of a Working Group to formulate definitions of competition, consumer trust and consumer choice and possible metrics for the future AoC team to consider in its gTLD review. The Applicant understands this effort has not been adopted by the ICANN Board, but many of the proposed metrics may be used to gauge the Applicant's gTLD effectiveness and the gTLD program. The Applicant intends to track costs and benefit metrics to inform future studies and reviews. Proposed definitions are:

- Consumer Trust is defined as the confidence registrants and users have in the consistency of name resolution and the degree of confidence among registrants and users that a TLD Registry operator is fulfilling its proposed purpose and is complying with ICANN policies and applicable national laws.
- Consumer Choice is defined as the range of options available to registrants and users for domain scripts and languages, and for TLDs that offer choices as to the proposed purpose and integrity of their domain name registrants.
- Competition is defined as the quantity, diversity, and the potential for

market rivalry of TLDs, TLD Registry operators, and Registrars.

Promoting Competition
Given the proposed definition for competition, the Applicant will attain this by contributing to the quantity and diversity within the Registry Operator space. The Applicant is a new entrant enhancing competition among the providers. The Applicant will promote competition for Registrants by amongst other things:

- Building a healthy growth trend of domain registrations
- Measure migration of content from other TLDs
- Maintain competitive pricing of domains

Promoting consumer trust
.charity will be developed with consumer trust and satisfaction in mind. After 2 years of operations, the Applicant will conduct a survey to measure consumer trust and consumer satisfaction. This will be used to improve the service. The Applicant will among other things measure the following:

- Service Availability of Critical Registry Systems
- Abuse and Takedown incidents
- Rights protection incidents
- WHOIS data accuracy

Promoting consumer choice
The Applicant intends to promote consumer choice by achieving the following:

- Display of registration requirements and restrictions in the gTLD
- Highly available and geographically diverse Registrar channel
- Effective sunrise and trademark services

Domain names will be available globally, although the Applicant’s initial marketing efforts will be predominately directed to potential Registrants represented by the six (6) official languages of the United Nations (“UN Languages”), Arabic, Chinese (Mandarin), English, French, Russian and Spanish.
After the initial 2 years it is the Applicant’s aim that:

- Registrants globally should have access to Registrar services for the gTLD in at least the six UN Languages
- The gTLD is offered by Registrars covering at least 40 Countries and territories globally

Information on the effectiveness of safeguards
The Applicant takes rights protection and abuse prevention and mitigation very seriously and has developed policies accordingly. Amongst others, the Applicant will collect and evaluate data regarding:

- Effectiveness of the Sunrise process in limiting abusive registration practices
- Effectiveness of the additional Abuse Prevention and Mitigation (″APM″)and Rights Protection Mechanisms (″RPM″)in limiting abusive registration practices
- Effectiveness of the mandatory APMs and RPMs

-end-

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

Q18b
How do you expect that your proposed gTLD will benefit Registrants, Internet users, and others?

The Applicant’s primary intention is to provide a favorable ecosystem for the growth and evolution of the sector. The key to achieving this aim are significant provisions for brand integrity and protection of intellectual property. The Applicant intends to push the boundaries of what can be done through innovative design of the new top level domain, including technologies that capitalize on the sector’s needs. A close relationship with the sector’s stakeholders is essential to this purpose, and will enable .charity to grow in response to both Registrant and user needs. The gTLD also contains significant opportunities as a next generation organizational scheme for online content, including provisions for abuse prevention to defend users against malicious registrations. The gTLD has been meticulously designed by a team of industry leaders from an array of different fields. This has enabled the creation of an airtight financial strategy, an inspired technological development plan as well as a close and dynamic relationship with the sector community - all critical needs on the path to the enduring success of the gTLD.

18(b)(i) What is the goal of your proposed gTLD in terms of areas of specialty, service levels, or reputation?

Specialty

The Applicant’s key specialty goal is to enable a secure and stable gTLD dedicated to providing global Internet users with a targeted space for subject matter of interest. This gTLD will serve as a home for both Registrants and end-users who feel an affinity with this sector and its associated content. Consequently they will prefer to register domain names, create and post content and seek information in a highly targeted manner.

Allowing users the ability to create a targeted, unique space within the new gTLD will enable them to customize their online offering and presence. The .charity gTLD will by itself clearly signal the nature and purpose of such websites to Internet users.

The applicant intends to actively promote gTLD specific vertical searching in the gTLD for the benefit of Registrants, end-users and other stakeholders. This specialization through Vertical Search will also benefit Internet users seeking authentic online information and products or services as they will no longer have to wade through content completely unrelated to their desired results.

As the gTLD is sector specific it will provide a better context for second level strings allowing for a much higher number of relevant and more conscise domains. This more targeted environment will simplify the user experience across multiple platforms specifically with smartphones and tablets where minimal input is favoured.

Service Levels

The goal of the gTLD Registry is to offer domain name registration services of the highest level, exceeding both ICANN requirements and current sector norms. To achieve these goals, the Applicant has contracted with well established, proven service providers offering the highest possible level of quality in Registry and Registrar services. The expertise of the service providers will ensure that the security and quality of the gTLD will be uncompromised.

The Applicant will further provide the highest level of service to trademark, legal rights owners and second-level domain owners. To achieve this goal the Applicant will be implementing a range of Abuse Prevention and Mitigation policies and procedures. The Applicant is also firmly committed to the protection of Intellectual Property rights and will implement all the mandatory Rights Protection Mechanisms (RPMs) contained in the Applicant Guidebook. Aswell as these The Applicant will further protect the rights of others through the implementation of additional RPMs. The RSP’s experience will ensure that the gTLD provides this high level of service to trademark and other legal rights owners to combat abusive and malicious activity within the gTLD.

The Registry will respond to abuse or malicious conduct complaints on a 24⁄7⁄365 basis, respond to requests from governmental and quasi-governmental agencies and law enforcement in a timely manner, and promptly abide by decisions and judgments of UDRP and URS panels, in accordance with ICANN consensus policies.

The Applicant will also provide fast and responsive (24⁄7⁄365) customer support to both Registrars and end-users in a number of languages to assist with general enquiries as well as complaints of abusive or malicious conduct.

Service Levels related to Registry Backend Services

The Applicant will work with Neustar Inc. (hereinafter “RSP”) whose extensive experience spans more than a decade. This will ensure delivery of the protected, trusted, and permanently-running Registry infrastructure necessary to reliably host and operate a gTLD. The Applicant will also work with its Registrars to ensure that consumers receive secure, fast, and reliable domain name registration services with a high-level of customer service.

The global DNS network that will be utilised for the resolution of domains in this gTLD has already been operating for over 10 years. It currently delivers DNS resolution for several TLD customers and provides low latency query responses with a 100% DNS uptime service level agreement.

The Applicant will further leverage the RSP’s existing DNSSEC infrastructure, capabilities, and experience to provide a robust and standards compliant implementation that ensures DNSSEC services are always available as part of the DNS.

The Shared Registry System (“SRS”) to be used for the Applicant’s gTLD is a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that has been designed to operate at the highest performance levels. The Applicant’s RSP has been able to meet or exceed their SLA requirements nearly every month since it’s inception. Their Registry has achieved a 99.997% success rate in meeting SLAs since 2004.

The Applicant’s RSP has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the gTLDs that it operates as a Registry Operator for both gTLDs and ccTLDs. The RSP’s thick WHOIS solution is production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years.

The Applicant will comply with all the data escrow requirements documented in the Registry Data Escrow (“RyDE”) Specification of the Registry Agreement and has a contract in place with Iron Mountain Intellectual Property Management, Inc. (“IM”) for RyDE Services. The Applicant and its RSP will in conjunction with Iron Mountain work to ensure that the escrow deposit process is compliant 100% of the time.

Reputation

The Applicant will ensure that the Registry enjoys an excellent reputation through its core focus on creating a secure, sustainable, and specialized gTLD, thus supporting ICANN’s primary goals for the new gTLD program in promoting consumer trust, consumer choice, competition and innovation.

The Applicant will strive to become a reputable and successful new gTLD by providing secure, fast and reliable customer service throughout the registration life cycle of all domains in the gTLD.

The Applicant will endeavour to ensure that only non-fraudulent Registrants have domain names in the gTLD via a WHOIS that is searchable, thick and reliable and by being highly responsive to complaints from legal rights owners. The Applicant will further implement an industry leading range of Abuse Prevention and Mitigation policies and procedures as well as RPMs.

The Applicant will provide the financial and operational stability to protect Registrants and ensure the reputation of the Registry. The Applicant has estimated the maximum costs of the critical functions for a three year period by taking the largest single year cost estimate (year 5) and multiplying this by 3. If the calculation used a lower figure the costs estimate would not be at the potential highest amount during the 5 years and the COI instrument would be too small in order to fund the costs of the 5 critical functions for at least 3 years.

The Applicant has decided to commit to providing the highest level of protection to Registrants and Stakeholders by providing ICANN with a COI for the maximum amount as recommended by ICANN in its COI Guidance. This ensures the Registry is reputable, remains conservative and mirrors ICANN’s core objectives. In a worst case scenario where the Applicant will not receive any revenue Registrants will be protected not only by the COI, but also by the fact that the Applicant has enough capital to operate for over 3 years.

Question 18(b)(ii) What do you anticipate your proposed gTLD will add to the current space, in terms of competition, differentiation, or innovation?

It is expected that .charity will provide significant competition for existing and forthcoming gTLDs. The .charity gTLD will provide a blank canvas of second level domains that will inevitably lead to increased consumer choice and significant innovation from the sector. It will allow Registrants to seek new and varied ways to separate themselves from the competition.

Competition

The Applicant will enhance competition by allowing new Registrants to create new online products and services serving the global marketplace and connecting geographically diverse Registrants and users with a common affinity for the specialized subject matter exemplified by the new gTLD. The new gTLD process and its resulting gTLDs are likely to incentivize top-level domains to improve the security and quality of their online products and services as well as introducing new ones. Thus, this gTLD will benefit consumers by increasing the likelihood of new innovative online products and services.The addition of a new gTLD such as .charity will also increase competition between existing registries.

The Applicant will promote competition to the benefit of the Registrants by amongst other things:

- Building a healthy growth trend of domain registrations to validate the specialty space
- Promote the migration of sector relevant content from other TLDs
- Maintaining competitive pricing of domains

Differentiation

Currently, there is no gTLD available on the Internet that signifies the specialized products, services, and subject matter encompassed by this gTLD. The gTLD string itself will give a clear indication to website visitors that the site has content relevant to the sector. This will result in the gTLD becoming globally recognizable and viewed as a trusted source of goods, services and information.

Innovation

The gTLD will demonstrate innovation through cutting edge RPMs.

Firstly the Applicant considers the Protection of Intergovernmental Organization (″IGO″) names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The Applicant will reserve these strings and only allow for their future release if an IGO on the “reserve list” wishes to make use of the protected string in the gTLD and provides the Applicant with sufficient documentation.

Secondly, the Applicant will require that Registrants agree to the Registry’s “Abuse and Rights Protection” Terms and Conditions as part of the registration process for the second-level domain, which includes displaying the APM Seal on the homepage. The APM Seal will provide users and legal rights holders with a direct link to an Abuse Prevention and Mitigation Report Website which will provide instructions on how to report abusive conduct to the Registry and law enforcement.

Finally if a Registrant during sunrise and landrush applies to register a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard it will receive a Capital City Claims (“CCC”) notification stating this. Subsequently they will have to reply unconditionally agreeing to comply with requirements to protect the reputation of the capital city and any further terms.

These functions will enhance Internet stability, security and will demonstrate to Registrars, Registrants, and end-users of the Registry that abusive or malicious conduct will not be tolerated. They will further contribute significantly to the integrity of the gTLD enabling an environment where stakeholders can innovate with confidence.

Question 18(b)(iii) What goals does your proposed gTLD have in terms of user experience?

The Applicant’s goals for the new gTLD are to provide a trusted, secure, and user friendly environment whereby domain names and content relating to its specific affinity group can flourish.

The Applicant believes that the success of the gTLD will be determined by the sector’s key stakeholders globally. The Applicant believes that stakeholders should have the opportunity to influence the gTLD and the way it is governed. Accordingly, the Applicant is establishing a Governance Council (“GC”), to serve as an advisory body.

.charity will be developed with consumer trust, choice and satisfaction in mind and after the initial 2 years, the Applicant will conduct a survey to analyse the gTLD′s success in these areas to help further improve the user experience.

To ensure a high level of service the Applicant will further measure:

- Service Availability Targets for the Critical Registry Functions
- The number of abuse incidents and takedowns
- ICANN Compliance

- Rights protection incidents (i.e. UDRP and URS)
- WHOIS data accuracy

The Applicant intends to promote consumer choice by providing the following:

- Highly available and geographically diverse Registrar distribution channel;
- Effective sunrise and trademark services.

Question 18(b)(iv) Provide a complete description of the applicant's intended registration policies in support of the goals listed above.

Registration Policies

The purpose and goal of the Applicant's policies are to ensure competition, fairness, trust and reliability for Registrars, Registrants, the user community, and other stake holders, while maintaining security and stability for the gTLD.

General Policy

Aside from certain start-up mechanisms, all domain names will generally be registered on a first-come, first-served basis. A Trademark Claims service will be offered for the first 90 days of general registration, with the intent of providing clear notice to potential Registrants of the existing rights of trademark owners with registered trademarks in the Trademark Clearinghouse.

Registration Policies

As per ICANN's requirements, the Applicant will be operating both a Sunrise and Landrush period ahead of general availability for the gTLD.

Governance Council

The Applicant is establishing a the GC, to be comprised of key sector stakeholders that will serve as an advisory body. Each GC will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific registration policies,the formulation of guidance on intellectual property and other best practices related to the gTLD.

The Applicant aims to develop an Abuse Prevention and Mitigation Working Group in conjunction with the GC. It will give the Applicant's team advice on abuse preventions and mitigation and how this may effect registration policies. The group will meet to regularly discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them.

Question 18(b)(v) Will your proposed gTLD impose any measures for protecting the privacy or confidential information of Registrants or users? If so, please describe any such measures.

Data and Privacy Policies

The Applicant shall comply with all the Data, WHOIS, and Privacy requirements in the Applicant Guidebook required by ICANN. The Applicant will take all possible steps to maintain the security and privacy of information or data that it may collect in connection with the planned function and usage of names domains, and will remain in compliance with all confidentiality and security regulations in relevant jurisdictions. This data will be held by the Applicant in accordance with the Registry Agreement that the Applicant will execute with ICANN.

The Applicant has further ensured that its suppliers also understand that keeping information secure and private is of crucial importance and will take all available steps to maintain the security and privacy of information collected from the Applicants in the Sunrise, Landrush and General Availability Phases.

Question 18(b) Describe whether and in what ways outreach and communications will help to achieve your projected benefits.

The Applicant plans on making the gTLD the premier gTLD where individuals and organizations can register, build and maintain websites relating to their specific interest area. Thus, communication with the public and development of an outreach campaign are important goals in connection with the gTLD.

During the gTLD evaluation process, the Applicant plans to conduct a two-to-three month communications campaign aimed at reaching sector stakeholders and informing them of the gTLD's mission and the opportunity to participate in the GC. The communication outreach will include email communications to hundreds of leading sector organizations. It will also be accompanied by the launch of a website for communicating information about the gTLD and allowing interested members of the related sector to express interest in serving on the GC. Other communications efforts, including but not limited to, press releases and social media campaigns may all be initiated to raise further awareness regarding the gTLD.

Shortly after completing the evaluation process and being awarded the gTLD, the Applicant will institute marketing and outreach efforts to inform the public about the new gTLD, its launch schedule, and its intended affinity group. The Applicant will use different outreach and communications methods and venues to get the new gTLD mission and message out to the public, including but not limited to the following: online and print press releases, communications with various media outlets, domain name sector groups, mobile apps and various social media platforms. The GC will be used as a further means of outreach and communication to the Internet community.
-end-

18(c). What operating rules will you adopt to eliminate or minimize social costs?

Q18C
What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)? What other steps will you take to minimize negative consequences⁄costs imposed upon consumers?

The Applicant fully appreciates the concerns of ICANN, the GAC and other consumer protection authorities about the need to operate new gTLDs in ways that minimize social costs, consumer vulnerabilities as well as other time and financial resource costs. To achieve these goals this gTLD will not only employ the ICANN mandated minimum protections, but will also deploy the following innovative protection measures that will put the gTLD at the forefront of addressing these critical issues:

1) Abuse Prevention and Mitigation Policies and Procedures

The Applicant's core mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. To achieve this goal the

Applicant will be implementing a range of Abuse Prevention and Mitigation (″APM″) policies and procedures.

These Policies and Procedures will include: 1) gTLD APM Plan, 2) Policies and Procedures to Minimize Abusive Registrations ,3) Abuse Point of Contact, 4) Policies for Handling Complaints Regarding the Abuse Policies, 5) Acceptable Use Policy (“AUP”), 6) Proposed Measures for Removal of Orphan Glue Records, 7) Resourcing plans for the initial implementation of, and ongoing maintenance of, the APM initiatives, 8) Registry semi-annual WHOIS verification, 9) Regular monitoring of WHOIS registration data for accuracy and completeness, 10) Registrar WHOIS self-certification, 11) WHOIS data reminder process, 12) Establishing policies and procedures to ensure Registrar compliance, which may include audits, financial incentives, penalties, or other means, 13) Registrar verification of WHOIS, 14) Abuse Response Process, 15) Policies and procedures that define malicious or abusive behaviour, 16) Service Level Requirements for resolution regarding APM issues, 17) Service Level Requirements for Law enforcement requests regarding APM issues, 18) Coordination of APM efforts with sector Groups and Law Enforcement, 19) Rapid takedown and suspension, 20) Controls to Ensure Proper Access to Domain Functions, 21) Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests, 22) Enabling multiple, unique points of contact to request and⁄or approve update, transfer, and deletion requests, 23) Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted, 24) Additional Mechanism for Protection of Capital City Names, 25) Additional Mechanisms to Protect and Reserve IGO Names, 26) Governance Council Structure, 27) Efforts to increase Registrant Security Awareness, 28) Registrant Disqualification, 29) Restrictions on Proxy Registration Services, 30) Registry Lock, 31) APM Seal. (Q28 for detail)

2) Rights Protection Mechanisms

The Applicant is firmly committed to the protection of Intellectual Property rights and to implementing all the mandatory Rights Protection Mechanisms (“RPMs”) contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. Use of domain names that infringe upon the legal rights of others in the gTLD will not be tolerated and preventing abusive registrations is a core objective of the Applicant. The nature of such uses creates security and stability issues for the Registry, Registrars, and Registrants, as well as for users of the Internet in general. The Applicant will minimize time or financial resources costs by preventing abusive registrations and reduce opportunities for behaviours such as phishing or pharming. This will be achieved by implementing comprehensive registration, anti-abuse, and rights protection guidelines as defined in its AUP, as well as innovative additional RPMs such as the Mechanism to Protect IGO Names by blocking second level labels currently present in the .int zone file and the Mechanism for Further Protection of Capital City Names, as described below. In order to identify and address the abusive use of registered names on an ongoing basis, the Applicant will also incorporate and abide by the following RPMs and all other RPMs as specified in Specification 7 of the Registry Agreement and as adopted by the ICANN Board of Directors as ICANN Consensus Policies.

These Rights Protection Mechanisms will among other things include: 1) Trademark Clearinghouse, 2) Applicant’s Sunrise Period, 3) Trademark Claims Service , 4) Uniform Domain Name Dispute Resolution Policy, 5) Uniform Rapid Suspension System, 6) Trademark Post-Delegation Dispute Resolution Procedure, 7) Mechanism to protect IGO Names, 8) Mechanism for Further Protection of Capital City Names, 9) Efforts to promote WHOIS Accuracy, 10) Thick Searchable WHOIS, 11) Semi Annual Audits to Ensure Accurate WHOIS, 12) Policies Handling Complaints Regarding Abuse and Rights Issues, 13) Registry Acceptable Use Policy (“AUP”), 14) Monitoring for Malicious Activity. (Q29 for detail)

3) Governance Council Structure

The Applicant believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed. Accordingly, the Applicant will establish a Governance Council (the “GC”) comprised of key sector stakeholders that will serve as an advisory body tasked with defining best practice recommendations for the gTLD space. The Applicant believes that the success of the gTLD will be determined largely by the sector’s key stakeholders. Not only will these stakeholders have the primary interest in registering domains in the gTLD, but they will also be motivated to protect the sector from practices that would negatively impact the sector overall. The GC exists to provide guidance on matters related to best practices, intellectual property, authentication, certification, and other matters of importance to the sector and it will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and other best practices related to the gTLD.

4) BITS and Coalition for Online Accountability (“COA”) Recommendations

The Applicant will further structure its policies around the BITS and COA Recommendations where relevant to this gTLD. The Applicant’s goal is to provide a safe and secure experience for consumers. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD’s reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial TLDs. The policy comprises of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial gTLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf].

The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy comprises of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http://bit.ly/HuHtmq.

We welcome the recommendations from BITS and the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

5) Registry Operators Startup Plan

The Applicant proposes to implement the following start-up plan so that the new gTLD is introduced in an orderly, transparent and stable manner. This will safeguard competition, fairness, trust and reliability for Registrants, the User Community, ICANN Accredited Registrars, and other Stakeholders.
The Applicant’s startup plan is designed to minimize social costs (e.g., time or financial resources costs, as well as various types of consumer vulnerabilities) by instilling a number of RPMs as well as APMs.
The plan consists of the following multi-phase process that will be executed by the Registry Operator. The timeline for the gTLDs start-up process and associated RPMs in the Applicants gTLD is as follows:

Phase 1 – Sunrise Process:

- Day 1: Sunrise round opens
- Day 60: Sunrise round Closes
- Day 61: Sunrise Allocation Including contention resolution mechanisms opens
- Day 71: Sunrise Allocation contention resolution mechanisms closes

• The following Rights Protection Mechanisms apply:
  a. Trademark Clearinghouse (“TMCH”)
  b. Sunrise Eligibility Requirements (“SER”)
  c. Sunrise Dispute Resolution Policy (“SDRP”)
  d. Uniform Domain Name Dispute Resolution Policy (“UDRP”)
  e. Uniform Rapid Suspension System (″URS”)
  f. Mechanism for the Protection of IGO Names (“PIN”)
  g. Trademark Claims Service (“TCS”) *

Phase 2 – Landrush process:

- Day 72: Landrush opens
- Day 102: Landrush closes
- Day 103: Landrush contention resolution mechanisms opens
- Day 113: Landrush contention resolution mechanisms closes

- The following Rights Protection Mechanisms apply:

  a. UDRP
  b. URS
  c. PIN
  d. Mechanism for Further Protection of Capital City Names (“CCC”)
  e. TCS *

Phase 3 – General Availability⁄Registrations:

- Day 114: General availability begins

- The following Rights Protection Mechanisms apply:

  a. UDRP
  b. URS
  c. PIN
  d. Trademark Post-Delegation Dispute Resolution Procedure (“PDDRP”)
  e. TCS for the 90 days after day 114 *

* To ease the concerns of trademark owners and mitigate the impact of infringing registrations, the Applicant will be implementing the TCS in all three phases of launch. It is important to note that during the General Availability Phase, the TCS will be used for 90 days, 30 days longer than the ICANN mandated minimum.

18(C)(i) How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come⁄first-serve basis?

Sunrise and Landrush periods:

During the gTLDs launch period, multiple applications for a particular domain name will be resolved through a Contention Resolution Mechanism (“CRM”) involving auctions. These CRMs will apply to the Sunrise and Landrush application phases. The CRMs will be conducted by Sedo GMBH, an experienced provider of domain auction services. The mechanisms offered will involve closed auctions where only specific bidders can participate.

During the Applicants Sunrise process, if there are two or more eligible applicants for one domain name string, then the contention will be resolved by auction. Auctions held during the Sunrise phase (“Sunrise Auctions”) will be closed and the only bidders will be eligible applicants according to the gTLDs Sunrise eligibility requirements including the TMCH.

During the Applicants Landrush process, if there are two or more eligible applicants for one domain name string, then the contention will be resolved by auction. Auctions held during the Landrush phase (“Landrush Auctions”) will be closed and the only bidders will be eligible applicants according to the gTLDs Landrush eligibility requirements.

General Availability:

After the two initial startup phases of the Registry the allocation of domain names will occur on a first-come first-serve basis, taking into account the registries APM and RPM mechanisms.

18(c)(ii) Explain any cost benefits for registrants you intend to implement (e.g., advantageous pricing, introductory discounts, bulk registration discounts).

Incentive, Marketing and Outreach Programs

The Applicant will implement a number of incentive, marketing assistance, awareness and PR programs to assist the Registrar channel in providing a sector leading experience to end-users and to provide cost benefits for registrants. The Applicant will work with the global Registrar channel to ensure that the new gTLD offer is clearly visible on registrar sites resulting in an increase in the awareness and in the number of new gTLD registrations. Achieving this visibility requires (1) a clear business case and incentives for registrars to motivate them and (2) mechanisms and assets to make it easy for them to do so.

The Applicant will at the time of launch depending upon market conditions consider incentive programs that will deliver cost benefits to registrants through either the use of advantageous pricing, introductory discounts, bulk registration discounts or other similar methods. The Applicant is aware of Specification 9 – Registry Operator Code of Conduct, and will not directly or indirectly show any preference or provide any special consideration to any Registrar in its marketing efforts.

Example incentive mechanisms the Applicant will provide to the registrars may include:

Marketing Incentives

The Applicant intends to provide expertise, tools and creative assets to the registrars as part of general marketing and co-marketing programs. There is a significant cost saving if the expertise, tools and assets are developed centrally and the costs amortized across the registrar base. Significant cost savings can occur relating to Market Research, Social Customer Relationship Management (“SCRM”), Content Management Systems (“CMS”), Direct Marketing Tools, Marketing Collateral and Analytics Solutions.

The Applicant will employ some or all of the following marketing techniques jointly with registrars globally: (1) Direct Response Print, (2) General Web Marketing, (3) Email campaigns without Incentive, (4) Email with Incentive, (5) Email Marketing - Prospect List, (6) Email Marketing - Sponsored Newsletter, (7) Direct Marketing with

Incentive, (8) Web Marketing with Incentive, (9) Viral Marketing (Social, Video, Micro-sites), (10) Develop User Interface Improvement best practices, (11) Develop Search Engine Optimization best practices, (12) Email Marketing - Registrar List
As an example of a marketing initiative, the Applicant will forward leads to the Registrars “buy” pages as an incentive via the means of Pay-Per-Click (“PPC”) search marketing. The Applicant will run multiple PPC campaigns targeting gTLD Registrants and point these to landing pages on the Registrar’s websites. Conversions are directly trackable from all PPC campaigns and keywords with a high Click-Through-Rate (“CTR”) or conversions will also be leveraged for SEO best practice purposes.

PR and Awareness Incentives:

In addition to the core outreach to the Registrar Channel, the Applicant will engage in a wider outreach to build awareness of the new gTLD with customers, end-users and other stakeholders. The Applicant will engage with a number of high profile individuals associated with the gTLD and will seek to reach end consumers through webcasts, podcasts, traditional broadcast TV as well as radio.

Provision of customer retention toolkits to Registrars:

The Applicant will use propensity modelling to build retention marketing programs to minimize churn whilst building renewal sustainability. The Applicant will develop econometric models designed to measure the likelihood of a customer segment to purchase a product or offer bundle, at a certain point in the relationship lifecycle. They are used to predict the best time, and the best combination of products, to offer to customers who match a certain profile. They are especially effective where there are large numbers of customers and reliable data can be gathered. The Applicant expects that registration volume in the gTLD will provide sufficient data for this modelling.

Measure, benchmark and improve the customer experience:

The Applicant will engage in a program to develop best practice policies related to the customer experience at differing levels of the channel. This will include the entire ecosystem from Registry through Registrar to Resellers and finally end-users. One key metric might be, for example, to reduce the number of clicks to make a purchase equivalent to the most customer friendly e-commerce sites in the world.
The Applicant might, for example, provide website performance tracking tools to registrars, which would benchmark current performance and provide insights into customers’ needs and behaviour at the point of purchase.
The Applicant will engage in a Social Customer Relationship Management Program to monitor social media feedback to questions, concerns or other issues. The Applicant will further seek to measure marketing communication expenditure and activity.

Other initiatives that will be considered by the Applicant in its outreach efforts:

(a) Customized Vertical Search App for major mobile platforms.
(b) Designated Twitter channel for the stakeholder community.
(c) Social Media outreach through Facebook and other social media solutions.

Translation into other languages:

At present, the Applicant plans to translate marketing collateral and other content that it considers to have geographically diverse appeal in to the 6 official UN languages, namely Arabic, Chinese (Mandarin), English, French, Russian and Spanish.

18(c)(iii) Note that the Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than ten years. Additionally, the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation? If so, please describe your plans.

The Applicant will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator has in excess of ten years of experience managing numerous gTLDs that utilize standard and unique business rules and lifecycles.

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. For the avoidance of doubt, the registration term for registered names may not exceed ten (10) years. Further the renewal of registered names may be made in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, renewal of registered names may not extend their registration period beyond ten (10) years from the time of the renewal.

The Applicant plans to review domain name registration rates on an annual basis and will make a determination at that time regarding adjustments, depending upon market factors. Thus, at this time, the Applicant does not plan to make specific guarantees regarding pricing increases.

The Applicant will provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the gTLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying or other programs which had the effect of reducing the price charged to registrars, unless such refunds, rebates, discounts, product tying or other programs are of a limited duration that is clearly and conspicuously disclosed to the registrar when offered) that complies with the requirements as outlined in the New gTLD Registry Agreement.
-end-

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

Q22
Introduction

The Applicant is aware of the substantial amount of work and effort that has gone into developing policy to address the issue of the reservation and release of geographic names under new gTLDs, including the valuable input from ICANN’s Governmental Advisory Committee (”GAC”), the Generic Names Supporting Organisation Reserved Names Working

Group, Registry Operators and from elsewhere within the ICANN community.

The Applicant is aware of and understands the requirements set forth in the 11 January 2012 version of the New gTLD Applicant Guidebook (New gTLD Applicant Guidebook) and the GAC advice for protection of geographic names and will implement appropriate measures to ensure that it complies in all respects with ICANN policies and rules regarding both the reservation and release of geographic names at the second level (or other levels).

In addition to this, the Applicant proposes to implement an additional mechanism for the protection of capital city names at the second level that exceeds the requirements in the New gTLD Applicant Guidebook. See description of Capital City Claim service described below.

Reservation of Geographic Names

The initial GAC advice on the protection of geographic names is contained in the GAC document “Principles Regarding New gTLDs” which was presented by the GAC on 28 March 2007. Section 2.7(a) of this document states that new gTLD applicants should “adopt, before the new gTLD is introduced, appropriate procedures for blocking, at no cost and upon demand of governments, public authorities or IGOs, names with national or geographic significance at the second level of any new gTLD”.

Specification 5 of the New gTLD Registry Agreement provides further clarity and details the Schedule of Reserved Names at the Second Level (or other levels) in gTLD Registries, whereby the Registry Operator undertakes to reserve certain domain names and prevent them from being registered, delegated or used.

Section 2 of Specification 5 of the New gTLD Registry Agreement requires that all two character labels are initially reserved. This is to avoid conflicts and confusion with existing ccTLD extensions.

Section 5 of Specification 5 of the New gTLD Registry Agreement is more comprehensive and states that:

“5. 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, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union 〈http:⁄⁄www.iso.org⁄iso⁄support⁄country_codes⁄iso_3166_code_lists⁄iso-3166-1_decoding_table.htm#EU〉 ;

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”.

In order to meet these requirements regarding country and territory names, the applicant will maintain and regularly update copies of the aforementioned internationally recognized lists. All labels appearing on those lists, and on any list promulgated or recognized by ICANN for reservation in the future, assuming the corresponding string is unregistered, The Applicant will afford the same protections to new states or cities as they are formed.

The Applicant will reserve all labels appearing on the above referenced lists from time to time, and prevent registration, delegation or use of such names in accordance with ICANN requirements and as described above. In order to ensure that this is implemented correctly, all such labels will be reserved in the name of the applicant in order to prevent their delegation and use.

Release of Reserved Geographic Names

Specification 5 of the New gTLD Registry Agreement also contains provisions for the release of country and territory names on the basis that agreement is reached with "the applicable government(s), provided, further, that Registry Operator may also propose release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN".

As such the applicant's proposed policy for the release of such reserved terms is cognisant of the review and approval process from the GAC and ICANN.

Based upon a review of the available literature, documentation and guidance, the applicant proposes the following policy to ICANN and the GAC for the potential release of reserved terms under the TLD:

i) Further to the successful evaluation and delegation of the TLD all of the aforementioned labels, as specified under Section 5 of Specification 5 of the New gTLD Registry Agreement will be reserved and thus unavailable for registration during each stage of the launch process including, but not limited to the Sunrise period, the Landrush period through to General registrations.

ii) At any stage during the launch process through to General registrations and beyond, the aforementioned reserved names may only be assigned to the relevant Government or public authority. In such situation they would be assigned using the following process:

a) The corresponding Government or public authority submits a request to the GAC seeking the assignment of the reserved name to themselves and provides the details of the proposed registrant entity for the domain name registration.

b) The GAC will validate it and authenticate the request to establish that is a genuine bona fide request.

c) Once this has been established by the GAC, the request for delegation will be forwarded to the applicant to request the assignment of the domain name. Simultaneously the GAC will also notify ICANN of the GAC approval of the request for the assignment of the domain name.

d) The applicant will issue a unique authorisation code to the proposed registrant entity.

e) The proposed registrant entity will then be able to request the assignment of the domain name to themselves using the authorisation code with an ICANN accredited registrar for the applicant TLD.

In addition to the above, the applicant will also adhere to and implement ICANN policy with regards to the reservation and release of such terms as and when required.

Additional Mechanism for Further Protection of Capital City Names

In parallel with the Landrush Period defined in the answer to question 18, the applicant will implement a Capital City Claim (“CCC”) service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is described below:

a) Any prospective domain name registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will automatically receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name corresponds to a capital city name of a country or territory listed in the ISO 3166-1 standard.

b) A potential domain name registrant receiving a CCC notification will have to send a response to the Applicant whereby it will unconditionally comply with the requirements as to representations and warranties required by the Applicant.

c) Unconditional acceptance of the representations and warranties set out in the CCC notification will be a material requirement for a prospective registrant to be eligible to register the domain name in question should said prospective registrant be successful in the Landrush period.

d) Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification listing the names in writing to the GAC Chair.
(see Q28 for more detail)
-end-

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

Q23
23.1 Introduction

The Applicant has elected to partner with Neustar, Inc to provide back-end services for the TLD registry. In making this decision, the Applicant recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the TLD registry. The following section describes the registry services to be provided.

23.2 Standard Technical and Business Components

Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. The Applicant will use Neustar’s Registry Services platform to deploy the TLD registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to this TLD:
- Registry-Registrar Shared Registration Service (SRS)
- Extensible Provisioning Protocol (EPP)
- Domain Name System (DNS)
- WHOIS

- DNSSEC
- Data Escrow
- Dissemination of Zone Files using Dynamic Updates
- Access to Bulk Zone Files
- Dynamic WHOIS Updates
- IPv6 Support
- Rights Protection Mechanisms
- Internationalized Domain Names (IDN).

The following is a description of each of the services.

SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.

EPP
The TLD registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.

DNS
The Applicant will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.

WHOIS
Neustar's existing standard WHOIS solution will be used for the TLD. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy and is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:
Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)
DNSSEC

An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question 43.

Data Escrow
Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:
- Protect against data loss
- Follow industry best practices
- Ensure easy, accurate, and timely retrieval and restore capability in the event of a

hardware failure
- Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.
Dissemination of Zone Files using Dynamic Updates
Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.

Access to Bulk Zone Files
The Applicant will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.

Dynamic WHOIS Updates
Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

IPv6 Support
The TLD registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS⁄DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.

Required Rights Protection Mechanisms
The Applicant, will provide all ICANN required Rights Mechanisms, including:
- Trademark Claims Service
- Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
- Registration Restriction Dispute Resolution Procedure (RRDRP)
- UDRP
- URS
- Sunrise service.

More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.

23.3 Unique Services
The Applicant will not be offering services that are unique to this TLD.

23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.
-end-

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24

24.1 Introduction

The Applicant has partnered with Neustar, Inc, an experienced TLD registry operator, for the operation of the TLD Registry. The Applicant is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.
The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

High-level SRS System Description

The SRS to be used for TLD will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, The Applicant is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:
- State-of-the-art, production proven multi-layer design-
- Ability to rapidly and easily scale from low to high volume as a TLD grows
- Fully redundant architecture at two sites
- Support for IDN registrations in compliance with all standards
- Use by over 300 Registrars
- EPP connectivity over IPv6
- Performance being measured using 100% of all production transactions (not sampling).

SRS Systems, Software, Hardware, and Interoperability

The systems and software that the registry operates on are a critical element to providing a high quality of service. If the systems are of poor quality, if they are difficult to maintain and operate, or if the registry personnel are unfamiliar with them, the registry will be prone to outages. Neustar has a decade of experience operating registry infrastructure to extremely high service level requirements. The infrastructure is designed using best of breed systems and software. Much of the application software that performs registry-specific operations was developed by the current engineering team and as a result the team is intimately familiar with its operations.

The architecture is highly scalable and provides the same high level of availability and performance as volumes increase. It combines load balancing technology with scalable server technology to provide a cost effective and efficient method for scaling.

The Registry is able to limit the ability of any one registrar from adversely impacting other registrars by consuming too many resources due to excessive EPP transactions. The system uses network layer 2 level packet shaping to limit the number of simultaneous connections registrars can open to the protocol layer.

All interaction with the Registry is recorded in log files. Log files are generated at each layer of the system. These log files record at a minimum:

- The IP address of the client
- Timestamp
- Transaction Details
- Processing Time.

In addition to logging of each and every transaction with the SRS Neustar maintains audit records, in the database, of all transformational transactions. These audit records allow the Registry, in support of the applicant, to produce a complete history of changes for any domain name.

SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:

- Protocol Layer
- Business Policy Layer
- Database.

Each of the layers is described below.

Protocol Layer

The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.

The EPP servers authenticate against a series of security controls before granting service, as follows:

- The registrar’s host exchanges keys to initiate a TLS handshake session with the EPP server.
- The registrar’s host must provide credentials to determine proper access levels.
- The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.

Business Policy Layer

The Business Policy Layer is the “brain” of the registry system. Within this layer, the policy engine servers perform rules-based processing as defined through configurable attributes. This process takes individual transactions, applies various validation and policy rules, persists data and dispatches notification through the central database in order to publish to various external systems. External systems fed by the Business Policy Layer include backend processes such as dynamic update of DNS, WHOIS and Billing.

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process

every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes.
The SRS today processes over 30 million EPP transactions daily.

Database
The database is the third core component of the SRS. The primary function of the SRS database is to provide highly reliable, persistent storage for all registry information required for domain registration services. The database is highly secure, with access limited to transactions from authenticated registrars, trusted application-server processes, and highly restricted access by the registry database administrators. A full description of the database can be found in response to Question 33.

Figure 24-1 depicts the overall SRS architecture including network components.

Number of Servers
As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the TLD registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.
Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:
- WHOIS
- DNS
- Billing
- Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for TLD.
The SRS includes an "external notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

WHOIS External Notifier
The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs

to change in WHOIS. See response to Question 26 for greater detail.
DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.
Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse
The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.
Frequency of Synchronization between Servers

The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.
Synchronization Scheme (e.g., hot standby, cold standby)
Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.

Compliance with Specification 6 Section 1.2
The SRS implementation for TLD is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.
Compliance with Specification 10
Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the TLD Registry.The following section describes Neustar’s experience and its capabilities to meet the requirements in the new agreement.

To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics.These measurements are key indicators of the performance and health of the registry. Neustar's current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.

24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:
- Development⁄Engineering
- Database Administration
- Systems Administration
- Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.

The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31.Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the TLD registry. The following resources are available from those teams:
Development⁄Engineering – 19 employees
Database Administration- 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees

The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the TLD registry.
-end-

25. Extensible Provisioning Protocol (EPP)

Q25
25.1 Introduction
The Applicant's back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries.
They deployed one of the first EPP registries in 2001 with the launch of .biz. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure that the Applicant is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the TLD registry.
This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.

25.2 EPP Interface

Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry.

However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.

The main features of the EPP implementation are:

- Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.
- Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
- Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
- Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
- Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
- Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
- Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.

25.3 Compliance with RFCs and Specifications

The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar’s ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.

EPP Toolkits

Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit

(SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.

The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol.The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a “dummy” server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.3 Proprietary EPP Extensions
The TLD registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the TLD registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.

The full EPP schema to be used in the TLD registry is attached in the document titled “EPP Schema.”

25.4 Resourcing Plans
The development and support of EPP is largely the responsibility of the Development⁄Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development⁄Engineering – 19 employees
Quality Assurance - 7 employees.

These resources are more than adequate to support any EPP modification needs of the TLD registry.
-end-

26. Whois

Q26
26.1 Introduction
The Applicant recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. The Applicant’s back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs,

ccTLDs and back-end registry services provider. As one of the first “thick” registry operators in the gTLD space, Neustar’s WHOIS service has been designed from the ground up to display as much information as required by a TLD and respond to a very stringent availability and performance requirement.

Some of the key features of the solution include:

• Fully compliant with all relevant RFCs including 3912
• Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years
• Exceeds current and proposed performance specifications
• Supports dynamic updates with the capability of doing bulk updates
• Geographically distributed sites to provide greater stability and performance
• In addition, the thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).

26.2 Software Components
The WHOIS architecture comprises the following components:
• An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.
• Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.
• Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.
• Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.
• Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.
• Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.
• Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization
• SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10
Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.
Table 26-1 describes Neustar’s compliance with Specifications 4 and 10.
Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

26.4 High-level WHOIS System Description

26.4.1 WHOIS Service (port 43)
The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves. The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name’s UTF-8 encoded representation along with the Unicode code page.

26.4.2 Web Page for WHOIS queries
In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application. It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:
• Domain names
• Nameservers
• Registrant, Technical and Administrative Contacts
• Registrars
It also provides features not available on the port 43 service.These include:
1. Redemption Grace Period calculation: Based on the registry’s policy, domains in pendingDelete can be restorable or scheduled for release depending on the date⁄time the domain went into pendingDelete. For these domains, the web based WHOIS displays “Restorable” or “Scheduled for Release” to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources
As described above the WHOIS architecture uses a workflow that decouples the update process from the SRS.This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar’s geographically diverse WHOIS sites use:
• Firewalls, to protect this sensitive data
• Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
• Packetshaper for source IP address-based bandwidth limiting
• Load balancers to distribute query load
• Multiple WHOIS servers for maximizing the performance of WHOIS service.
The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
Figure 26-1 depicts the different components of the WHOIS architecture.

26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, “Technical Overview”, when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer.The update agent processes these updates, transforms the data if necessary and then uses messaging oriented middleware to publish all updates to each WHOIS slave.The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.

26.7 Frequency of Synchronization between Servers Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish⁄subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% = 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% = 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.

26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will include precautions to avoid abuse and will enable users to search the WHOIS directory using any one or more of the following fields:

- Domain name
- Registrar ID
- Contacts and registrant's name
- Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)
- Name server name and name server IP address
- The system will also allow search using non-Latin character sets which are compliant with IDNA specification.

The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
Figure 26-2 shows an architectural depiction of the new service.

To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:

- Data Mining
- Unauthorized Access
- Excessive Querying
- Denial of Service Attacks

To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:

- Username-password based authentication
- Certificate based authentication
- Data encryption
- CAPTCHA mechanism to prevent robo invocation of Web query
- Fee-based advanced query capabilities for premium customers.

The searchable WHOIS application will adhere to all privacy laws and policies of the Applicant's registry.

26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:

- Development⁄Engineering – 19 employees
- Database Administration – 10 employees
- Systems Administration – 24 employees
- Network Engineering – 5 employees

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's

WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the Applicant's registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

27. Registration Life Cycle

Q27
27.1 Registration Life Cycle
Introduction
The Applicant will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be used for the TLD.
Domain Lifecycle - Description
The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts
Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the Applicant's registry per the defined TLD business rules.
The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.
- OK – Default status applied by the Registry.
- Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.
- PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the TLD registry.
- PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.
- PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.
- PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the Applicant's registry.
- PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in the TLD registry.
  Hold   Removes the domain from the DNS zone
- UpdateProhibited – Prevents the object from being modified by an Update command.
- TransferProhibited – Prevents the object from being transferred to another Registrar by the Transfer command.
- RenewProhibited – Prevents a domain from being renewed by a Renew command.
- DeleteProhibited – Prevents the object from being deleted by a Delete command.
The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above.Upon registration a domain will either

be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:

- Domain may be updated
- Domain may be deleted, either within or after the add-grace period
- Domain may be renewed at anytime during the term
- Domain may be auto-renewed by the Registry
- Domain may be transferred to another registrar.

Each of these actions may result in a change in domain state. This is described in more detail in the following section. Every domain must eventually be renewed, auto-renewed, transferred, or deleted. A registrar may apply EPP statuses described above to prevent specific actions such as updates, renewals, transfers, or deletions.

27.1.1 Registration States

Domain Lifecycle – Registration States

- As described above the Applicant’s registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:
- Active
- Inactive
- Locked
- Pending Transfer
- Pending Delete.

All domains are always in either an Active or Inactive state, and throughout the course of the lifecycle may also be in a Locked, Pending Transfer, and Pending Delete state.Specific conditions such as applied EPP policies and registry business rules will determine whether a domain can be transitioned between states. Additionally, within each state, domains may be subject to various timed events such as grace periods, and notification periods.

Active State

The active state is the normal state of a domain and indicates that delegation data has been provided and the delegation information is published in the zone. A domain in an Active state may also be in the Locked or Pending Transfer states.

Inactive State

The Inactive state indicates that a domain has not been delegated or that the delegation data has not been published to the zone. A domain in an Inactive state may also be in the Locked or Pending Transfer states. By default all domain in the Pending Delete state are also in the Inactive state.

Locked State

The Locked state indicates that certain specified EPP transactions may not be performed to the domain. A domain is considered to be in a Locked state if at least one restriction has been placed on the domain; however up to eight restrictions may be applied simultaneously. Domains in the Locked state will also be in the Active or Inactive, and under certain conditions may also be in the Pending Transfer or Pending Delete states.

Pending Transfer State

The Pending Transfer state indicates a condition in which there has been a request to transfer the domain from one registrar to another. The domain is placed in the Pending Transfer state for a period of time to allow the current (losing) registrar to approve (ack) or reject (nack) the transfer request. Registrars may only nack requests for reasons specified in the Inter-Registrar Transfer Policy.

Pending Delete State
The Pending Delete State occurs when a Delete command has been sent to the Registry after the first 5 days (120 hours) of registration. The Pending Delete period is 35-days during which the first 30-days the name enters the Redemption Grace Period (RGP) and the last 5-days guarantee that the domain will be purged from the Registry Database and available to public pool for registration on a first come, first serve basis.

27.1.2 Typical Registration Lifecycle Activities
Domain Creation Process
The creation (registration) of domain names is the fundamental registry operation. All other operations are designed to support or compliment a domain creation. The following steps occur when a domain is created.
1. Contact objects are created in the SRS database. The same contact object may be used for each contact type, or they may all be different. If the contacts already exist in the database this step may be skipped.
2. Nameservers are created in the SRS database. Nameservers are not required to complete the registration process; however any domain with less than 2 name servers will not be resolvable.
3. The domain is created using the each of the objects created in the previous steps.In addition, the term and any client statuses may be assigned at the time of creation.
The actual number of EPP transactions needed to complete the registration of a domain name can be as few as one and as many as 40. The latter assumes seven distinct contacts and 13 nameservers, with Check and Create commands submitted for each object.

Update Process
Registry objects may be updated (modified) using the EPP Modify operation.The Update transaction updates the attributes of the object.
For example, the Update operation on a domain name will only allow the following attributes to be updated:
- Domain statuses
- Registrant ID
- Administrative Contact ID
- Billing Contact ID
- Technical Contact ID
- Nameservers
- AuthInfo
- Additional Registrar provided fields.

The Update operation will not modify the details of the contacts. Rather it may be used to associate a different contact object (using the Contact ID) to the domain name. To update the details of the contact object the Update transaction must be applied to the contact itself. For example, if an existing registrant wished to update the postal address, the Registrar would use the Update command to modify the contact object, and not the domain object.
Renew Process
The term of a domain may be extended using the EPP Renew operation. ICANN policy in general establishes the maximum term of a domain name to be 10 years, and the Applicant will not deviating from this policy. A domain may be renewed ⁄ extended at any point time, even immediately following the initial registration.The only stipulation is that the overall term of the domain name may not exceed 10 years. If a Renew operation is performed with a term value will extend the domain beyond the 10 year limit, the Registry will reject the transaction entirely.
Transfer Process
The EPP Transfer command is used for several domain transfer related operations:
- Initiate a domain transfer
- Cancel a domain transfer

- Approve a domain transfer
- Reject a domain transfer.

To transfer a domain from one Registrar to another the following process is followed:

1. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
2. If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into pendingTransfer status
3. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar’s message queue
4. The domain remains in pendingTransfer status for up to 120 hours, or until the losing (current) Registrar Acks (approves) or Nack (rejects) the transfer request
5. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer
6. The requesting Registrar may cancel the original request up until the transfer has been completed.

A transfer adds an additional year to the term of the domain. In the event that a transfer will cause the domain to exceed the 10 year maximum term, the Registry will add a partial term up to the 10 year limit. Unlike with the Renew operation, the Registry will not reject a transfer operation.

Deletion Process

A domain may be deleted from the SRS using the EPP Delete operation. The Delete operation will result in either the domain being immediately removed from the database or the domain being placed in pendingDelete status. The outcome is dependent on when the domain is deleted. If the domain is deleted within the first five days (120 hours) of registration, the domain is immediately removed from the database. A deletion at any other time will result in the domain being placed in pendingDelete status and entering the Redemption Grace Period (RGP). Additionally, domains that are deleted within five days (120) hours of any billable (add, renew, transfer) transaction may be deleted for credit.

27.1.3 Applicable Time Elements

The following section explains the time elements that are involved.

Grace Periods

There are six grace periods:

- Add-Delete Grace Period (AGP)
- Renew-Delete Grace Period
- Transfer-Delete Grace Period
- Auto-Renew-Delete Grace Period
- Auto-Renew Grace Period
- Redemption Grace Period (RGP).

The first four grace periods listed above are designed to provide the Registrar with the ability to cancel a revenue transaction (add, renew, or transfer) within a certain period of time and receive a credit for the original transaction.

The following describes each of these grace periods in detail.

Add-Delete Grace Period

The APG is associated with the date the Domain was registered.Domains may be deleted for credit during the initial 120 hours of a registration, and the Registrar will receive a billing credit for the original registration.If the domain is deleted during the Add Grace Period, the domain is dropped from the database immediately and a credit is applied to the
Registrar’s billing account.

Renew
Delete Grace Period

The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may be deleted for credit during the 120 hours after a renewal.The grace period is intended to allow Registrars to correct domains that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP (see below).

Transfer-Delete Grace Period
The Transfer-Delete Grace Period is associated with the date the Domain was transferred to another Registrar. Domains may be deleted for credit during the 120 hours after a transfer. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP. A deletion of domain after a transfer is not the method used to correct a transfer mistake. Domains that have been erroneously transferred or hijacked by another party can be transferred back to the original registrar through various means including contacting the Registry.

Auto-Renew-Delete Grace Period
The Auto-Renew-Delete Grace Period is associated with the date the Domain was auto-renewed. Domains may be deleted for credit during the 120 hours after an auto-renewal.The grace period is intended to allow Registrars to correct domains that were mistakenly auto-renewed. It should be noted that domains that are deleted during the auto-renew delete grace period will be placed into pendingDelete and will enter the RGP.

Auto-Renew Grace Period
The Auto-Renew Grace Period is a special grace period intended to provide registrants with an extra amount of time, beyond the expiration date, to renew their domain name.The grace period lasts for 45 days from the expiration date of the domain name. Registrars are not required to provide registrants with the full 45 days of the period.

Redemption Grace Period
The RGP is a special grace period that enables Registrars to restore domains that have been inadvertently deleted but are still in pendingDelete status within the Redemption Grace Period. All domains enter the RGP except those deleted during the AGP.
The RGP period is 30 days, during which time the domain may be restored using the EPP RenewDomain command as described below. Following the 30day RGP period the domain will remain in pendingDelete status for an additional five days, during which time the domain may NOT be restored.The domain is released from the SRS, at the end of the 5 day non-restore period. A restore fee applies and is detailed in the Billing Section. A renewal fee will be automatically applied for any domain past expiration.
Neustar has created a unique restoration process that uses the EPP Renew transaction to restore the domain and fulfill all the reporting obligations required under ICANN policy. The following describes the restoration process.

27.2 State Diagram
Figure 27-1 provides a description of the registration lifecycle.
The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:
- Create: Registry receives a create domain EPP command.
- WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
- WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.
- Remove Nameservers: Domain’s nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.

- Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
- Delete: Registry receives a delete domain EPP command.
- DeleteAfterGrace: Domain deletion does not fall within the add grace period.
- DeleteWithinAddGrace: Domain deletion falls within add grace period.
- Restore: Domain is restored. Domain goes back to its original state prior to the delete command.
- Transfer: Transfer request EPP command is received.
- Transfer Approve⁄Cancel⁄Reject: Transfer requested is approved or cancel or rejected.
- TransferProhibited: The domain is in clientTransferProhibited and⁄or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.

DeleteProhibited: The domain is in clientDeleteProhibited and⁄or serverDeleteProhibited status.This will cause the delete command to fail. The domain goes back to its original state.
Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.

27.2.1 EPP RFC Consistency
As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.
27.3 Resources
The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development⁄Engineering team, with testing performed by the Quality Assurance team. Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The Applicant's registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development⁄Engineering - 19 employees
Registry Product Management - 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

28. Abuse Prevention and Mitigation

Q28
The Applicant's core mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. To achieve this goal the Applicant will be implementing a range of Abuse Prevention and Mitigation policies and procedures. The following is an overview of initiatives undertaken by the Applicant:

1.   gTLD Abuse Prevention and Mitigation Implementation Plan

1 gTLD Abuse Prevention and Mitigation Implementation Plan

The Applicant will be implementing a thorough and extensive Abuse Prevention and Mitigation plan, designed to minimise abusive registrations and other detrimental activities that may negatively impact internet users. This plan includes the establishment of 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 gTLD through all Registrars of record, including those involving a reseller. Details of this point of contact will be clearly published on the Applicant's website.

Strong abuse prevention for a new gTLD is an important benefit to the internet community. The Applicant and its backend services provider agree that a Registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the Registry’s stakeholders’ interest. The Applicant’s Backend Services Provider brings extensive experience establishing and implementing registration policies. This experience will be leveraged to help the Applicant combat abusive and malicious domain activity within the new gTLD space.

One of the key functions of a responsible domain name Registry includes working towards the eradication of domain name abuse including, but not limited to, those resulting from:

- Illegal or fraudulent actions
- Spam
- Phishing
- Pharming
- Distribution of malware
- Fast flux hosting
- Botnets
- Illegal distribution of copyrighted material
- Distribution of child pornography
- Online sale or distribution of illegal pharmaceuticals.

Further explanation of behaviour considered to be abusive can be found in the Acceptable Use Policy (“AUP”) below. Any second-level domain found to be facilitating such behaviours, either upon registration or subsequently, will be subject to rapid compliance action as per the policies outlined below.

The Applicant believes that the success of the gTLD will be determined largely by the sector’s broad-spectrum of key stakeholders, who operate globally. The Applicant believes that these stakeholders will be motivated to protect the sector from detrimental practices. The Applicant further believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed, including its abuse prevention policies where appropriate. Accordingly, the Applicant is establishing a Governance Council, to be comprised of key sector stakeholders that will serve as an advisory body. The Governance Council will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and the formulation of guidance on other best practices related to the gTLD. The Applicant aims to develop an Abuse Prevention and Mitigation Working Group in conjunction with the GC. It will give the Applicant’s team advice on abuse preventions and mitigation and how this may effect registration policies. The group will meet to regularly discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them. Registrants, Registrars and the Registry will all be involved in this working group.This will likely prove important as the battle with abusive behaviour online must continuously evolve given that abusive behaviour itself mutates and changes. The Governance Council will offer significantly greater opportunities to identify emerging threats and rapidly establish procedures to deal with them than might have been possible simply with a Registry perspective.

2 Policies and Procedures to Minimize Abusive Registrations

Regardless of how well intentioned its user-base is, a Registry must have the policies, resources, personnel, and expertise in place to combat abusive DNS practices. The Applicant’s Registry Backend Services Provider is at the forefront of the prevention of such abusive practices. We also believe that a strong program is essential given that Registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet, often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name Registrant, but also to millions of unsuspecting Internet users.

Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. The Applicant has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the Registry.

Coalition for Online Accountability (“COA”) Recommendations

The Applicant will further structure its policies around the COA Recommendations where relevant to this gTLD. The Applicant’s goal is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD’s reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy is comprised of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http://bit.ly/HuHtmq. We welcome the recommendations from the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

BITS Recommendations

The Applicant will further structure its policies around the BITS Recommendations where relevant to this gTLD. The Applicant’s goal is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD’s reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial gTLDs. The policy is comprised of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial gTLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf]. We welcome the recommendations from SSWG and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

2.1 Implementation plan for Abuse Point of Contact

As required by the Registry Agreement, The Applicant will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive matters requiring expedited attention. The Applicant will provide a timely response to abuse complaints concerning all names registered in the gTLD by registrars and their resellers. The Applicant will also provide such information to ICANN prior to the delegation of any domain names in the gTLD. This information shall consist of, at a minimum, a valid name, e-mail address dedicated solely to the handling of malicious conduct complaints and a telephone number and mailing address for the primary contact. The Applicant will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited Registrars, the Applicant’s Registry Backend Services Provider shall have an additional point of contact, as it does today, handling requests by Registrars related to abusive domain name practices.

2.2 Policies for Handling Complaints Regarding the Abuse Policies

In order to operate under the new gTLD, Registrants must accept the Acceptable Use Policy. The new gTLD Registry’s Acceptable Use Policy clearly delineates the types of activities that constitute “abuse” and the repercussions associated with an abusive domain name registration. In addition, the policy will be incorporated into the applicable Registry-Registrar Agreement (“RRA”) and reserve the right for the Registry to take the appropriate actions based on the type of abuse. This will include locking down the domain name preventing any changes to the contact and name server information associated with the domain name, placing the domain name “on hold” rendering the domain name non-resolvable, transferring the domain name to another Registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation. When appropriate, the Applicant will also share information with law enforcement. Each ICANN and gTLD accredited Registrar must agree to pass the Acceptable Use Policy on to its Resellers (if applicable) and ultimately to the gTLD Registrants. The Registry’s initial Acceptable Use Policy that the Applicant will use in connection with the gTLD is outlined in a section below.

2.3 Proposed Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (“SSAC”) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the “dominant use of orphaned glue supports the correct and ordinary operation of the DNS.” See http://www.icann.org/en/committees/security/sac048.pdf.
While orphan glue records often support the correct and ordinary operation of the DNS, we understand that such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, botnets, malware, and other abusive behaviours. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS.
Thus, the Registry Operator will remove orphan glue records (as defined at the above link) when provided with evidence in written form that such records are present in connection with malicious conduct. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.
To prevent orphan glue records, the Registry Backend Services Provider performs the following checks before removing a domain or name server:

Checks during domain delete:
- Parent domain delete is not allowed if any other domain in the zone refers to the child name server.
- If the parent domain is the only domain using the child name server, then both the domain and the glue record are removed from the zone.

Check during explicit name server delete:
- The Registry Backend Services Provider confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:
- If the parent domain references the child name server AND if other domains in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain goes out of the zone but the name server glue record does not.

- If no domains reference a name server, then the glue record is removed from the zone file.

2.4 Resourcing plans for the initial implementation of, and ongoing maintenance of, the Abuse Prevention and Mitigation initiatives

Details related to resourcing plans for the initial implementation and ongoing maintenance of the Applicant’s abuse plan are provided in Section 7 of this response.

3 Measures to promote WHOIS accuracy both directly by the Registry and by Registrars via requirements in the Registry-Registrar Agreement (“RRA”):

The Applicant acknowledges that ICANN has developed a number of mechanisms over the past decades that are intended to address the issue of inaccurate WHOIS information. Such measures alone have not proven to be sufficient and the Applicant will offer a mechanism whereby third parties can submit complaints directly to the Applicant about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or any other action was taken. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, the Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies. Further efforts to pre-empt inaccurate WHOIS data made by the Applicant will include:

1) The Applicant will in general discourage the use of proxy registration services. The Applicant understands that there are instances when proxy registrations may be required and will develop best practices for when these instances occur.
2) The Applicant will maintain a web-based form for third parties to submit claims regarding false and⁄or inaccurate WHOIS data and the Applicant will forward credible claims to the Registrar for investigation⁄resolution. The Applicant will follow up to verify that the claim has been satisfactorily resolved. Failure of the Registrar or the Registrant to resolve the problem may result in the Applicant placing the domain name on hold, except in extraordinary circumstances.
3) The Applicant’s Registry Backend Services Provider will regularly remind Registrars of their obligation to comply with ICANN’s WHOIS Data Reminder Policy. This policy requires Registrars to validate the WHOIS information provided during the registration process, to investigate claims of fraudulent WHOIS information, and to cancel domain name registrations for which WHOIS information is determined to be invalid.
4) WHOIS Verification by Registrars. As part of their Registry-Registrar Agreement all accredited Registrars will be required to revalidate WHOIS data for each record they have registered in the gTLD. The Applicant will leave the ultimate determination of how this procedure takes place to the Registrar, but it must include one of the following approved methods. (1) Email notification (2) Outbound telemarketing effort to the individual listed as the administrative contact for the domain.

3.1 Regular monitoring of registration data for accuracy and completeness

As part of their Registry-Registrar Agreement, all of the Applicant’s Registrars will be required to revalidate WHOIS data for each record they have registered on a bi-annual basis. This revalidation will require the Registrar to notify its Registrants in the gTLD about this requirement. While the Applicant reserves the right to suspend

domain names that are not verified in a timely manner, the Applicant will engage in other outreach to the Registrant prior to suspending any domain name. As part of the gTLD Abuse reporting system, users can report missing or incomplete WHOIS data via the Registry website. The Applicant will also perform randomized audits of verified WHOIS information to ensure compliance and accuracy.
The Applicant's selected Registry Backend Services Provider has established policies and procedures to encourage Registrar compliance with ICANN's WHOIS accuracy requirements..

3.2 Registrar WHOIS policy self-certification and authentication

The self-certification program consists, in part, of evaluations applied equally to all operational ICANN accredited Registrars for the gTLD and is conducted from time to time throughout the year. Process steps are as follows:
The Registry Backend Services Provider sends an email notification to the ICANN primary Registrar contact, requesting that the contact go to a designated URL, log in with his⁄her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.
When the form is submitted, the Registry Backend Services Provider sends the Registrar an automated email confirming that the form was successfully submitted.
The Registry Backend Services Provider reviews the submitted form to ensure the certifications are compliant.
The Registry Backend Services Provider sends the Registrar an email notification if the Registrar is found to be compliant in all areas.
If a review of the response indicates that the Registrar is out of compliance or if the Registry Backend Services Provider has follow-up questions, the Registrar has 10 days to respond to the inquiry.
If the Registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, the Registry Backend Services Provider sends the Registrar a Breach Notice and gives the Registrar 30 days to cure the breach.
If the Registrar does not cure the breach, the Registry Backend Services Provider may terminate the Registry-Registrar Agreement (RRA).

3.3 WHOIS data reminder process.

The Registry Backend Services Provider regularly reminds Registrars of their obligation to comply with ICANN's WHOIS Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http:⁄⁄www.icann.org⁄en⁄Registrars⁄wdrp.htm). The Registry Backend Services Provider sends a notice to all Registrars once a year reminding them of their obligation to be diligent in validating the WHOIS information provided during the registration process, to investigate claims of fraudulent WHOIS information, and to cancel domain name registrations for which WHOIS information is determined to be invalid.

3.4 Establishing policies and procedures to ensure Registrar compliance with policies, which may include audits, financial incentives, penalties, or other means.

The Applicant will require as part of the RRA obligations that all accredited Registrars for the gTLD participate in the abuse prevention and mitigation procedures and policies, as well as efforts to improve the accuracy and completeness of WHOIS data. In addition, the Applicant will work to develop an economic incentive program, such as Market Development Funds for Registrars who meet certain SLAs for performance in this area.

3.5 Registry bi-annual WHOIS verification

Additionally, the Applicant will, of its own volition and no less than twice per year, perform a manual review of a random sampling of gTLD domain names in its Registry to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, the Applicant will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their Registrants. Thirty days (30) after forwarding the complaint to the Registrar, the Applicant will reexamine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or some other action was taken. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, The Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

3.6 Registrar bi-annual verification of WHOIS

The Applicant will require in the Registry-Registrar Agreement that all accredited Registrars in this gTLD will be obliged to verify WHOIS data for each record they have registered in the gTLD twice a year. Verification can take place via email, phone or any other method to confirm the accuracy of the WHOIS data associated with the domain name. The Applicant will randomly audit WHOIS records to ensure compliance and accuracy. As part of the gTLD Abuse reporting system, users can report missing or incomplete WHOIS data via the Registry website.

4 Policies and procedures that define malicious or abusive behaviour

The applicant has developed policies and procedures that define malicious and abusive behaviour. More information on these policies and procedures can be found in section 14 - Acceptable Use Policy.

4.1 Service Level Requirements for resolution of APM related activities

As pertains to the Applicant’s service level requirements for resolution, we aim to address and potentially rectify the issue as it pertains to all forms of abuse and fraud within 24 hours. Once abusive behaviour is detected or reported, the Applicant’s Customer Service center immediately creates a support ticket in order to monitor and track the issue through resolution. This support team is operational 24⁄7⁄365. A preliminary assessment will be performed in order to determine whether the abuse claim is legitimate. We will classify each incidence of legitimately reported abuse into one of two categories based on the probable severity and immediacy of harm to Registrants and Internet users.

Category 1:

- Probable Severity or Immediacy of Harm: Low
- Examples of types of abusive behaviour: Spam, Malware
- Mitigation steps:
  - Investigate
  - Notify Registrant
- Response times – up to 3 days depending on severity.

Category 2:

- Probable Severity or Immediacy of Harm: Medium to High
- Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control
- Mitigation steps:

- Suspend domain name
- Investigate
- Restore or terminate domain name

- Response times - up to 1 day.

4.2 Service Level Requirements and Coordination regarding Law enforcement APM requests

With the assistance of its Registry Backend Services Provider, the Applicant will meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement, governmental and quasi-governmental agencies of illegal conduct in connection with the use of the gTLD. The Registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such a response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by the Applicant for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by the Registry and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring Registrar is then given 24 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 24-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on "ServerHold".

4.3 Coordination with sector Groups and Law Enforcement

One of the reasons for which the Registry Backend Services Provider was selected to serve as the Registry Backend Services Provider by the Applicant is the Registry Backend Services Provider's extensive experience and its close working relationship with a number of law enforcement agencies.

The Registry Backend Services Provider is also a participant in a number of sector groups aimed at sharing information amongst key sector players about the abusive registration and use of domain names. Through these organizations the Registry Backend Services Provider shares information with other registries, Registrars, ccTLDs, law enforcement, security professionals, etc. Not only on abusive domain name registrations within its own gTLDs, but also provides information uncovered with respect to domain names in other registries. The Registry Backend Services Provider has often found that rarely are abuses found only in the gTLDs which it manages, but also within other gTLDs. The Registry Backend Services Provider routinely provides this information to the other registries so that it can take the appropriate action.

When executed in accordance with the Registry Agreement, plans will result in compliance with contractual requirements.

The Applicant believes that the proposed collection of protections that involve both proactive and reactive mechanisms outlined above will provide an unmatched level of security and anti-abuse activity within the gTLD. These mechanisms will be part of both the Registry-Registrar Agreement as well as the Registrant Registration Agreement.

4.4 Rapid takedown and suspension system

The Applicant is committed to ensuring that the use of the internet within its Registry is compliant with all relevant laws and legal directions.

The Applicant notes that its role as the Registry operator is not one of judge and jury in all jurisdictions and as such shall direct all complainants to the legal process in the relevant jurisdiction. Upon receiving a valid and enforceable legal judgment or direction it shall comply forthright with the appropriate action which shall include rapid takedown and⁄or suspension.

5 Controls to Ensure Proper Access to Domain Functions

5.1 Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests;

To ensure proper and secure access to domain functions, the Applicant will develop best practices for its Registrars relating to enabling its Registrants to utilize two factor authentication in its interaction with their Registrar and ultimately the Registry.
The goal of these best practices is to improve domain name security and assist Registrars in protecting the accounts they manage by providing another level of assurance that only authorized registrants can communicate through the registrar with the Registry.

5.2 Enabling multiple, unique points of contact to request and⁄or approve update, transfer, and deletion requests;

The Applicant will investigate the costs and benefits for introducing a service whereby a Registrant can elect to designate multiple points of contact for each domain registered to approve changes to a domain before they are effectuated. The Applicant is of the opinion that these additional checks could improve the security of each domain and will look for ways to deploy them in the most cost-effective and user-friendly manner possible.

5.3 Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted

The Applicant will investigate the costs and benefits for introducing a service where by a Registrant can elect to designate multiple points of contact for each domain registered to receive notification of changes to a domain when they are effectuated. The Applicant is of the opinion that these additional checks could improve the security of each domain and will look for ways to deploy them in the most cost-effective and user-friendly manner possible.

6. Additional Abuse Prevention and Mitigation initiatives

6.1 Additional Mechanism for Protection of Capital City Names

In parallel with the Landrush Period defined in the answer to question 18, the Applicant will implement a Capital City Claim ("CCC") service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is as follows:

1. Any prospective domain name Registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name corresponds to a capital city name of a country or territory listed in the ISO 3166-1 standard.
2. A potential domain name Registrant receiving a CCC notification will have to send a response to the Applicant whereby it will unconditionally comply with the requirements as to representations and warranties required by the Applicant. This will protect the reputation of the capital city as well as any further relevant terms and conditions provided.
3. Unconditional acceptance of the warranties set out in the CCC notification will be a material requirement for a prospective Registrant to be eligible to register

the domain name in question should said prospective Registrant be successful in the Landrush period.

4. Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification in writing to the ICANN Government Advisory Committee (″GAC″) Chair.

6.2 Additional Mechanisms to Protect and Reserve IGO Names

The Applicant considers the Protection of Intergovernmental Organization (″IGO″) names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The .int domain is used for registering organizations established by international treaties between or among national governments and which are widely considered to have independent international legal personality. Thus, the names of these organizations, as with geographic names, can lend an official imprimatur, and if misused, be a source of public confusion or deception.

Reservation of IGO names:

In addition to the mandated and additional reservation of geographic names as provided for in response to Question 22, the Applicant will reserve, and thereby prevent registration of, all names that are registered as second level domains in the most recent .int zone as of 1st November 2012. By doing so, the Applicant will extend additional protection to IGOs that comply with the current eligibility requirements for the .int gTLD as defined at http:⁄⁄www.iana.org⁄domains⁄int⁄policy⁄, and that have obtained a second-level registration in the .int zone.

Release of IGO names:

In the future, should any of the IGOs wish to make use of the protected strings, the Registry will release and assign the domain to the respective IGOs using the following process:

a) The IGO submits a request to the Applicant in the hope of the reserved name being assigned to themselves and provides the necessary documentation and details of the proposed registrant entity for the domain name registration.
b) The Applicant will validate and authenticate the request to establish that it is a genuine bona fide request.
c) Once the request has been approved the Applicant will notify the requesting IGO as well as ICANN and the GAC of the approval for the assignment of the domain name.
d) The Applicant will issue a unique authorization code to the proposed IGO registrant.
e) The proposed IGO registrant will then be able to request that the assignment of the domain name is given to them using the authorization code with an ICANN and gTLD accredited Registrar of their choice.

6.3 Abuse Prevention and Mitigation Seal

The Applicant intends to further augment the security and stability of its gTLD by implementing the Abuse Prevention and Mitigation Seal (the “APM Seal”). The APM Seal will provide users and stakeholders in the sector with a one-click mechanism for how to access relevant Abuse Prevention and Mitigation processes. Registrants on the gTLD will be required to implement an APM Seal on their web pages that users can click-on and be taken to a web resource detailing the relevant mechanisms for how to report and address abuse on the gTLD. The Applicant will in cooperation with the Governance Council for the sector establish relevant procedures and processes that will be presented to stakeholders with potential grievances.

The APM Seal will operate as follows:

1. Registrant will be required to agree to the Registry's "Abuse and Rights Protection" Terms and Conditions as part of the Registration process for the second-level domain including clauses relating to the APM Seal.
2. The Terms and Conditions will require the Registrant to include the APM Seal in a prominent place on its website.
3. Following the registration, the Registry will automatically email the Registrant's Administrative, Technical, and Billing contacts with an additional notification that the APM Seal needs to be included on the Registrant's homepage. The Registrant has 120 days from the date of registration (the "Grace Period") to effectuate the fixing of the APM seal.
4. During the Grace Period, the domain registration will be flagged in WHOIS or a linked system as being in the APM Seal Grace Period.
5. When the APM Seal has been activated, the second-level domain will have the APM Seal marked as active in WHOIS or a linked system.
6. If the Registrant does not activate the APM Seal before the Grace Period expires, the site will be flagged as being out of the Grace Period for the APM Seal activation and the Registry will notify the Registrant's Administrative, Technical, and Billing contacts with an additional notification that this APM Seal activation is out of its Grace Period. The contacts will further be notified that the APM Seal must be included on the page and that the Registrant is granted a further 30 days before the site is flagged as being in breach of the Registration terms.
7. Should the Registrant fail to comply and activate the APM Seal within the period specified in the Acceptable Use Policy, the Registry will conduct an investigation on that domain. If after the investigation it is determined that the domain is in breach of the Acceptable Use Policy the Registry reserves the right to suspend and cancel the domain.
8. Exceptions: if a Registrant has a second-level domain that is:
(a) Used for forwarding to another domain
(b) The domain is not used for a website
(c) The domain is currently not in use, or
(d) There is another reason why the seal cannot technically be included

Should the domain be in any of the aforementioned states then the Registrant can activate the APM Seal stating that the domain is one of the exceptions (as listed above) and therefore does not need to include the APM Seal. If a site is listed to be in any of these exception states and then the use of the domain changes to a state that would require the APM Seal, the Registrant must then change the domains status to comply with Acceptable Use Policy. The Registry will conduct an investigation on that domain. If after the investigation it is determined that the domain is in breach of the Acceptable Use Policy the Registry reserves the right to suspend and cancel the domain.

6.4 Governance Council

The Applicant believes that the success of the gTLD will be determined in large by the gTLD's stakeholders. Not only will these stakeholders have the primary interest of registering domains on the gTLD, but they will also be motivated to protect the sector from practices that would negatively impact the sector overall. The Applicant further believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed. Accordingly, the Applicant is establishing a Governance Council (the "GC"), to be comprised of key sector stakeholders that will serve as an advisory body.

The GC will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and the formulation of guidance on intellectual property and other best practices related to the gTLD. This will lead the policy development process of defining how the APM Reporting Website should best reflect the options users, rights holders, etc., have for addressing infringing content or other issues.

7. Resource Planning

7.1 Resource Planning Specific to Backend Registry Activities

Responsibility for abuse mitigation rests with a variety of functional groups. The Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The customer service team also plays an important role in assisting with the investigations, responding to customers, and notifying Registrars of abusive domains. Finally, the Policy⁄Legal team is responsible for developing the relevant policies and procedures.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams globally distributed:

Customer Support – 12 people
Policy⁄Legal – 2 people
The resources are more than adequate to support the abuse mitigation procedures of the Registry.

7.2 Administrative Services Provider – Famous Four Media Limited

In addition to those resources set out above provided by the Registry's backend services provider the Applicant's Administration Services Provider shall provide the following extra resources:

- Sunrise Validation Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
- Ongoing Rights Protection Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.

The two key objectives of the Sunrise Validation Team and the Ongoing rights Protection Team (together the "Rights Team") is to:

a. Prevent abusive registrations; and
b. Identify and address the abusive use of registered names on an ongoing basis
Because rights protection is a fundamental core objective of the Applicant it has contracted with its Registry Administration Services Provider that the number of full time personnel made available to the Applicant will be 125% of the estimated requirement to ensure that at all times the Applicant is over resourced in this area. In addition the Applicant shall instruct outside Counsel in any relevant jurisdiction on all matters that are unable to be adequately dealt with by the Sunrise Validation Team or the Ongoing Rights Protection Team.

8. ICANN Prescribed Measures

In accordance with its obligations as a Registry operator, the Applicant will comply with all requirements in the 'gTLD Applicant Guidebook'. In particular, we will comply with the following measures prescribed by ICANN which serve to mitigate the potential for abuse in the gTLD:

- DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage Registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy-to-use manner in order to facilitate deployment by Registrants. Prohibition on Wild Carding as required by section 2.2 of Specification 6 of the Registry Agreement.

- Removal of Orphan Glue records (discussed above in section 4).

9. Increasing Registrant Security Awareness

In order to operate a secure and reliable gTLD, the Applicant will attempt to improve Registrant awareness of the threats of domain name hijacking, Registrant impersonation and fraud, and emphasise the need for and responsibility of Registrants to keep registration (including WHOIS) information accurate. Awareness will be raised by:

- Publishing the necessary information on the Abuse page of our Registry website in the form of presentations and FAQ's.
- Developing and providing to Registrants and resellers Best Common Practices that describe appropriate use and assignment of domain auth Info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

The increase in awareness renders Registrants less susceptible to attacks on their domain names owing to the adoption of the recommended best practices thus serving to mitigate the potential for abuse in the gTLD. The clear responsibility on Registrants to provide and maintain accurate registration information (including WHOIS) further serves to minimise the potential for abusive registrations in the gTLD.

10. Registrant Disqualification

Registrants, their agents or affiliates found through the application of the AUP to have repeatedly engaged in abusive registration may be disqualified from maintaining any registrations or making future registrations. This will be triggered when the Registry Backend Services Provider's records indicate that a Registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy. Registrant disqualification provides an additional disincentive for qualified Registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.

In addition, name servers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

For a Registrant to be placed on a list of bad actors, the Applicant will examine the factors noted above, and such determination shall be made by the Applicant at its sole discretion. Once the Applicant determines that a Registrant should be placed onto the list of bad actors, the Applicant will notify its Registry Backend Services Provider, who will be instructed to cause all of the Registrant's second-level domains in the gTLD to resolve to a page which notes that the domain has been disabled for abuse-related reasons. The second-level domains at issue will remain in this state until the expiration of the Registrant's registration term or a decision from a UDRP panel or court of competent jurisdiction requires the transfer or cancellation of such domains.

11. Restrictions on Proxy Registration Services

The Applicant will in general discourage the use of proxy registration services. The Applicant further understands that there are instances when proxy registrations may be required and will develop best practices when these instances occur. Whilst it is understood that implementing measures to promote WHOIS accuracy is necessary to ensure that the Registrant may be tracked down, it is recognised that some Registrants may wish to utilise a proxy registration service to protect their privacy. In the event that Registrars elect to offer such services, the following conditions apply:

- Registrars should take the best practice guidance developed by the Applicant and the Governance Council for the gTLD into account when making Proxy registration services available to its Registrants.
- Registrars must ensure that the actual WHOIS data is obtained from the Registrant and must maintain accurate records of such data.
- Registrars must provide Law Enforcement Agencies ("LEA") with the actual WHOIS data upon receipt of a verified request.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the Abuse page of the Registry website. Individuals and organisations will be encouraged through the Abuse page to report any domain names they believe violate the above restrictions, following which appropriate action may be taken by the Registry Backend Services Provider. Publication of these conditions on the Abuse page of the Registry website ensures that Registrants are aware that despite utilisation of a proxy registration service, actual WHOIS information will be provided to LEA upon request in order to hold Registrants liable for all actions in relation to their domain name.
The certainty that WHOIS information relating to domain names which draw the attention of LEA will be disclosed results in the gTLD being less attractive to those seeking to register domain names for abusive purposes, thus mitigating the potential for abuse in the gTLD.

12. Registry Lock

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. Whilst the Applicant will take efforts to promote the awareness of security amongst Registrants, it is recognised that an added level of security may be provided to Registrants by 'Registry locking' the domain name and thereby prohibiting any updates at the Registry operator level. The Registry lock facility will be offered to all Registrars who may request this service on behalf of their Registrants in order to prevent unintentional transfer, modification or deletion of the domain name. This facility mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update nameservers of a mission-critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name.
Upon receipt of a list of domain names to be placed on Registry lock by an authorised representative from a Registrar, the Registry Backend Services Provider will:

1. Validate that the Registrar is the Registrar of record for the domain names.
2. Set or modify the status codes for the names submitted to serverUpdateProhibited, serverDeleteProhibited and/or serverTransferProhibited depending on the request.
3. Record the status of the domain name in the Shared Registration System (SRS).
4. Provide a monthly report to Registrars indicating the names for which the Registry lock service was provided in the previous month.

13. Scope/Scale Consistency

The Applicant believes that the proposed collection of protections that involve both proactive and reactive mechanisms outlined above will provide an unmatched level of security and anti-abuse activity within the gTLD and is appropriate for the size and scale of the gTLD.

13.1 Scope⁄Scale Consistency Specific to Backend Registry Activities

The Registry Backend Services Provider is an experienced backend Registry provider that has developed and uses proprietary system scaling models to guide the growth of its gTLD supporting infrastructure. These models direct the Registry Backend Services Provider's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. The Registry Backend Services Provider periodically updates these models to account for the adoption of more capable and cost-effective technologies. The Registry Backend Services Provider's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, The Registry Backend Services Provider derived the necessary infrastructure required to implement and sustain this gTLD and its APM policies.

14. Acceptable Use Policy

This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its Registrar partners and⁄or that may put the safety and security of any Registrant or user at risk. The process also allows the Registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert the Registry's Registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

- Phishing; a criminal activity employing tactics to defraud and defame Internet users via sensitive information with the intent to steal or expose credentials, money or identities. A phishing attack often begins with a spoofed email posing as a trustworthy electronic correspondence that contains hijacked brand names e.g. (financial institutions, credit card companies, e-commerce sites). The language of a phishing email is misleading and persuasive by generating either fear and⁄or excitement to ultimately lure the recipient to a fraudulent Web site. It is paramount for both the phishing email and Web site to appear credible in order for the attack to influence the recipient. As with the spoofed email, phishers aim to make the associated phishing Web site appear credible. The legitimate target Web site is mirrored to make the fraudulent site look professionally designed. Fake third-party security endorsements, spoofed address bars, and spoofed padlock icons falsely lend credibility to fraudulent sites as well. The persuasive inflammatory language of the email combined with a legitimate looking Web site is used to convince recipients to disclose sensitive information such as passwords, usernames, credit card numbers, social security numbers, account numbers, and mother's maiden name.
- Malware; malicious software that was intentionally developed to infiltrate or damage a computer, mobile device, software and⁄or operating infrastructure or website without the consent of the owner or authorized party. This includes, amongst others, Viruses, Trojan horses, and worms.
- Domain Name or Domain Theft; the act of changing the registration of a domain name without the permission of its original Registrant.

- Botnet Command and Control; Services run on a domain name that is used to control a collection of compromised computers or “zombies,” or to direct Distributed Denial of Service attacks (“DDoS attacks”)
- Distribution of Malware; The intentional creation and intentional or unintentional distribution of “malicious” software designed to infiltrate a computer system without the owner’s consent, including, without limitation, computer viruses, worms, keyloggers, and Trojans.
- Fast Flux Attacks/Hosting; A technique used to shelter Phishing, Pharming, and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP addresses associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find.
- Hacking; the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Pharming; The redirecting of unknown users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Spam; The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the legal age in the relevant jurisdiction.
- Further abusive behaviours include, but are not limited to; Cybersquatting,Front-Running,Gripe Sites, Deceptive and/or Offensive Domain Names, Fake Renewal Notices,Cross-gTLD Registration Scam, Name Spinning, Pay-per-Click, Traffic Diversion, False Affiliation, Domain Kiting / Tasting, fast-flux and 419 scams.

The Registry reserves the right, at its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on Registry lock, hold or similar status, that it deems necessary, to its discretion; (1) to protect the integrity and stability of the Registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the Registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by the Registry or any Registrar in connection with a domain name registration. The Registry also reserves the right to place upon Registry lock, hold or similar status a domain name during resolution of a dispute.
Registrants must also agree that they will not use their domain for any purposes which are prohibited by the laws of the jurisdiction(s) in which they do business or any other applicable law. You may not use your domain for any purposes or in any manner which violate a statute, rule or law governing use of the Internet and/or electronic commerce, including those statutes related to gaming and/or online gambling.
In addition, The Applicant reserves the right to deny attempted registrations from repeat violators of the Registry’s Acceptable Use Policy. The Registry’s Acceptable Use Policy will incorporate a certification by the Registrant that the domain will be used only for licensed, legitimate activities, and not to facilitate piracy or infringements. The Registrant will be required to accept these terms as part of its registration agreement. The Applicant reserves the right to suspend or cancel a domain for violation of the Registry’s Acceptable Use Policy.

15. Abuse Response Process

The Registry is committed to ensuring that those domain names associated with abuse or

malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or are part of a real-time investigation by law enforcement.
Once a complaint is received from a trusted source, third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring Registrar will be notified and be given 48 hours to investigate the activity. This will result in either the take down of the domain name by placing the domain name on hold or the deletion of the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 48-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on “ServerHold”. Although this action removes the domain name from the gTLD zone, the domain name record still appears in the gTLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Additionally, the Applicant will require Registrars to adhere to the following abuse-prevention procedures:

- Each new gTLD accredited Registrar must provide and maintain a valid primary point of contact for abuse complaints. The Applicant will require this as part of the new gTLD RRA.
- The Applicant will explicitly define for Registrars what constitutes abusive behaviour including but not limited to, malicious, negligent, and reckless behaviour. The definition of abusive behaviour will be contained in the AUP and the Applicant will require this as part of the new gTLD RRA.
- Registrars must notify the Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc.), along with the gTLD impacted. This will be required as part of the new gTLD RRA.
- The Applicant will initiate an Abuse Prevention and Mitigation Working Group. This group will be developed in conjunction with the gTLD Governance Council mentioned above. Its aim will be to give the Applicant’s team alternate perspectives about handling incidents of abuse and ways to mitigate them. The group will meet regularly to discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them for the gTLD.

-end-

29. Rights Protection Mechanisms

Q29
The Applicant will be implementing an extensive range of Rights Protection Mechanisms (“RPMs”) designed to minimize abusive registrations and other activities that may affect the legal rights of others. The Applicant will implement and comply with all ICANN required RPMs and will in addition implement further measures to better protect the rights of others and minimize abusive registrations.

The following is an overview of Applicant’s response to Q29:

1. Rights Protection as a core objective
2. Plans for Rights Protection Mechanisms as part of Start-Up
3. ICANN Mandated Rights Protection Mechanisms
3.1. Trademark Clearinghouse (“TMCH”)

1 Rights Protection as a core objective
The Applicant is firmly committed to the protection of Intellectual Property rights and to implementing the mandatory RPMs contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. Use of domain names that infringe upon the legal rights of others in the gTLD will not be tolerated and preventing abusive registrations is a core objective of the Applicant. The nature of such uses creates security and stability issues for the Registry, Registrars, and Registrants, as well as for users of the Internet in general. The Applicant will prevent abusive registrations and reduce opportunities for behaviours such as phishing or pharming by implementing comprehensive registration, anti-abuse, and rights protection guidelines as defined in its AUP, as well as innovative additional RPMs such as PIN and the CCC, as described below. In order to identify and address the abusive use of registered names on an ongoing basis, the Applicant will also incorporate and abide by all mandated RPMs as specified in Specification 7 of the Registry Agreement and as adopted by the ICANN Board of Directors as ICANN Consensus Policies.

2 Plans for Rights Protection Mechanisms as part of Start-Up

The timeline for start-up RPMs in the Applicant′s gTLD is as follows:

Phase 1 – Sunrise Process:

- Day 1: Sunrise round opens
- Day 60: Sunrise round Closes
- Day 61: Sunrise Allocation including Contention Resolution Mechanisms (″CRM”) opens
- Day 71: Sunrise Allocation CRM closes

- The following Rights Protection Mechanisms apply:
  a. TMCH
  b. Sunrise Eligibility Requirements (“SER”)
  c. Sunrise Dispute Resolution Policy (“SDRP”)
  d. UDRP
  e. URS
  f. PIN
  g. TCS*

Phase 2 – Landrush process:

- Day 72: Landrush opens
- Day 102: Landrush closes
- Day 103: Landrush CRM opens
- Day 113: Landrush CRM closes

- The following Rights Protection Mechanisms apply:
  a. UDRP
  b. URS
  c. PIN
  d. CCC
  e. TCS*

Phase 3 – General Availability⁄Registrations:

- Day 114: General availability begins

- The following Rights Protection Mechanisms apply:
  a. UDRP
  b. URS
  c. PIN
  d. PDDRP
  e. TCS* (90 days)

* To ease the concerns of trademark owners and mitigate the impact of infringing registrations, the Applicant will be implementing the Trademark Claims service in all three phases of launch. It is important to note that during the General Availability Phase, the Trademark Claims service will be used for 90 days, 30 days longer than the ICANN mandated minimum.

3 ICANN Mandated Rights Protection Mechanisms

3.1 Trademark Clearinghouse (“TMCH”)
The first mandatory RPM required of each new gTLD Registry is support for, and interaction with, the TMCH. The TMCH is intended to serve as a central repository for information pertaining to the rights of trademark holders to be authenticated, stored, and disseminated. The data maintained in the clearinghouse will support and facilitate other RPMs, including the mandatory Sunrise Period and Trademark Claims service. Although the operational details of how the TMCH will interact with Registry operators and Registrars are still being developed by ICANN, the Applicant is actively monitoring the developments of the Implementation Assistance Group (“IAG”). The IAG is working with ICANN staff to refine and finalize the rules, procedures and technical requirements for the TMCH. In addition, the gTLD’s Registry Backend Services Provider is actively participating in the IAG to ensure that the protections afforded by the clearinghouse and associated RPMs are feasible, implementable, and well understood.

Utilizing the TMCH, the Applicant will offer: (i) a Sunrise registration service for 60 days during the pre-launch phase giving eligible trademark owners an early opportunity to register second-level domains in new gTLDs; and (ii) a TCS in all 3 phases of launch including 90 days after phase 3 general availability.

3.2 Applicant’s Sunrise Period (“ASP”)
All domain names registered during the Sunrise Period will be subject to the Applicant’s domain name registration policy. The Applicant will surpass ICANN’s mandated minimum by offering a Sunrise Period for sixty (60) days. Owners of trademarks listed in the TMCH that also meet the Applicant’s domain name registration requirements will be able to register domain names that are an identical match of

their listed trademarks. The Applicant has engaged Famous Four Media Limited (“FFM”) as well as other suppliers to assist with this process. The FFM Sunrise Validation Team will consist of a minimum of 11 employees who will work with the Applicant’s Trademark Validation Team (“TVT”) and outside counsel, to receive and authenticate all Sunrise registrations.

Registrars who are accredited to sell names in the gTLD will ensure that all Sunrise Registrants meet SERs, which will be verified by Clearinghouse data. The proposed SERs include: (i) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use – was submitted to, and validated by, the TMCH; or (b) that have been court-validated; or (c) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008, (ii) optional Registry-elected requirements regarding the international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon submission of all of the required information and documentation, the Registrar will forward the information to the Applicant’s TVT for authentication. The Applicant’s TVT will review the information and documentation and verify the trademark information and registration eligibility, and notify the potential registrant of any deficiencies.

The Applicant will also incorporate a SDRP. The SRDP will allow challenges to Sunrise Registrations by third parties after acceptance of the registration based on the following four grounds: (i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not have the necessary protections on or before the effective date of the Registry Agreement.

After receiving a Sunrise Complaint, the TVT will review the Complaint to see if the Complainant reasonably asserts a legitimate challenge as defined by the SDRP. If not, the TVT will send a notice to the Complainant that the complaint does not fall within one of the delineated grounds as defined by the SDRP and that the Applicant considers the matter closed.

If the domain name is found to not meet the SERs, the TVT will immediately suspend the domain name. Thereafter, the TVT will immediately notify the Sunrise Registrant of the suspension of the domain name, the nature of the complaint, and provide the registrant with the option to correct the SER deficiencies in a timely manner or the domain name will be cancelled.

If the registrant responds in a timely manner, the response will be reviewed by the TVT to determine if the SERs are met. If the TVT is satisfied by the registrant’s response, the TVT will submit a request to lift the suspension of the domain name and notify the Complainant that their dispute was denied. If the registrant does not respond in a timely manner, the TVT will then notify the Complainant that the complaint was upheld and the registration will be cancelled.

3.3 Trademark Claims Service
The Applicant will offer a TCS in Sunrise and Landrush as well as 90 days of general registration (30 days longer than the ICANN mandated minimum period.) The TCS will be

monitored by the TVT. Registrars who are accredited to sell names in the gTLD will be required to review all domain names requested to be registered during the Trademark Claims period to determine if they are an identical match of a trademark that has been filed with the TMCH. A domain name will be considered an identical match when the domain name consists of the complete and identical textual elements of the mark, and includes domain names where (a) spaces contained within a mark are either replaced by hyphens or omitted; (b) certain special characters contained within a trademark are spelled out with appropriate words describing it (e.g., @ and &); and (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain name are either (i) omitted or (ii) replaced by hyphens or underscores. Domain names that are plural forms of a mark or that merely contain a mark as a sub string will not qualify as an identical match.

If the Registrar determines that a prospective domain name registration is identical to a mark registered in the TMCH, the Registrar will be required to ensure that a “Trademark Claims Notice” (“Notice”) in English is sent to the prospective registrant of the domain name and a blind copy is sent to the Applicant’s TVT. The Notice will provide the prospective registrant with information regarding the trademark referenced in the notice to enhance understanding of the Trademark rights being claimed by the trademark holder. The Notice will be provided in real time without cost to the prospective registrant.

After sending the Notice, the Registrar will require the prospective registrant to specifically warrant within five (5) days that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the notice; and (iii) to the best of the prospective registrant’s knowledge that the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice. If the warranty satisfies these requirements, the Registrar will effectuate the registration and notify the Applicant’s TVT.

After the effectuation of a registration that is identical to a mark listed in the TMCH, the Registrar will be required to notify the trademark owner that a domain name representing the listed mark has been registered. A copy of this communication will also be sent to the TVT. The trademark owner then has the option of filing a Complaint under the UDRP and the URS against the domain name registrant. The Applicant will require in its relevant agreements that the Registry, Registrar, and registrant all submit to and abide by the determinations of the UDRP and the URS providers.

3.4 Uniform Domain Name Dispute Resolution Policy
The Applicant will abide by all decisions rendered by UdrpP providers and will specify in its Registry Registrar Agreement (″RRA″) and Registration Agreements (″RA″) that all parties must also abide by all decisions made by panels in accordance with the UDRP. On the Applicant’s Registry website, the Applicant will designate a Rights Protection Contact (“Rights Contact”) which will receive all UDRP Complaints and decisions. Upon receipt of a determination, the Rights Contact will work with technical staff at the Registry Backend Services Provider to temporarily lock any domain names as required, and will notify the appropriate Registrar to cancel or transfer all registrations determined by a UDRP panel to be infringing.

3.5 Uniform Rapid Suspension System
The Applicant will implement the URS as provided in the Applicant Guidebook. The Applicant will also specify in its RRA that all parties abide by all decisions made by panels in accordance with the URS. In response to complaints made by trademark owners that the UDRP was too cost prohibitive and slow, and that more than 70 percent of UDRP cases were “clear cut” cases of cybersquatting, ICANN adopted the Implementation Review Team’s (″IRT″) recommendation that all new gTLD registries be required, pursuant to their contracts with ICANN, to take part in a URS. The purpose of the URS

is to provide a more cost effective and timely mechanism for brand owners than the UDRP to protect their trademarks and to promote consumer protection on the Internet. The URS is not meant to address questionable cases of alleged infringement (e.g., use of terms in a generic sense) or for anti-competitive purposes or denial of free speech, but rather for those cases in which there is no genuine contestable issue as to the infringement and abuse that is taking place.

Unlike the UDRP which requires little involvement of gTLD registries, the URS envisages much more of an active role at the Registry-level. For example, rather than requiring the Registrar to lock down a domain name subject to a UDRP dispute, under the URS it is the Registry that must lock the domain within 24 hours of receipt of the complaint from the URS Provider to restrict all changes to the registration data, including transfer and deletion of the domain names.

The Rights Contact will receive all URS Complaints verified by the URS Provider and provide its contact information. In the event of a decision in favour of the complainant, the Registry is required to suspend the domain name. This suspension remains in effect for the remainder of the registration period and would not resolve the original website. The nameservers would be redirected to an informational web page describing the URS Process. The WHOIS for that domain will state that the domain name will not be able to be transferred, deleted, or modified for the life of the registration. Finally, there is an option for a successful complainant to extend the registration period for one additional year at commercial rates. Upon receipt of a decision in the registrant’s favour, Rights Contact will notify the Registry operator to unlock the domain name.

3.6 Trademark Post-Delegation Dispute Resolution Procedure (“PDDRP”)

The Applicant will participate in all post-delegation procedures required by the Registry agreement, including the PDDRP, and will abide by any decisions of any PDDRP Provider as required in Specification 7 of the Registry Agreement.

4 Additional Rights Protection Mechanisms to be implemented by the Applicant

4.1 Mechanism to Protect IGO Names

The Applicant considers the Protection of Intergovernmental Organization (″IGO″) names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The .int domain is used for registering organizations established by international treaties between or among national governments and which are widely considered to have independent international legal personality. Thus, the names of these organizations, as with geographic names, can lend an official imprimatur, and if misused, be a source of public confusion or deception.

Reservation of IGO names:

In addition to the mandated and additional reservation of geographic names as provided for in response to Question 22, the Applicant will reserve, and thereby prevent registration of, all names that are registered as second level domains in the most recent .int zone as of 1st November 2012. By doing so, the Applicant will extend additional protection to IGOs that comply with the current eligibility requirements for the .int gTLD as defined at http:⁄⁄www.iana.org⁄domains⁄int⁄policy⁄, and that have obtained a second-level registration in the .int zone.

Release of IGO names:

In the future, should any of the IGOs wish to make use of the protected strings, the Registry will release and assign the domain to the respective IGOs using the following process:

a)The IGO submits a request to the Applicant in the hope of the reserved name being

assigned to themselves and provides the necessary documentation and details of the proposed registrant entity for the domain name registration.
b)The Applicant will validate and authenticate the request to establish that it is a genuine bona fide request.
c)Once the request has been approved the Applicant will notify the requesting IGO as well as ICANN and the GAC of the approval for the assignment of the domain name.
d)The Applicant will issue a unique authorization code to the proposed IGO registrant.
e)The proposed IGO registrant will then be able to request that the assignment of the domain name is given to them using the authorization code with an ICANN and gTLD accredited Registrar of their choice.

4.2 Mechanism for Further Protection of Capital City Names
In parallel with the Landrush Period defined in the answer to question 18, the Applicant will implement a Capital City Claim (CCC) service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is as follows:
a)Any prospective domain name registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name matches a capital city name of a country or territory listed in the ISO 3166-1 standard.
b)A potential domain name registrant receiving a CCC notification will have to send a response to the Applicant whereby they will agree to unconditionally comply with requirements as to representations and warranties required by the Applicant in order to protect the reputation of the capital city as well as any further relevant terms and conditions provided.
c)Unconditional acceptance of the warranties set out in the CCC notification will be a material requirement for a prospective registrant to be eligible to register the domain name in question should said prospective registrant be successful in the Landrush period.
d)Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification in writing to the ICANN Government Advisory Committee (″GAC″) Chair.

4.3 Abuse Prevention and Mitigation Seal
The Applicant has developed an Abuse Prevention and Mitigation Seal (″APM Seal″) to further augment the security and stability of its gTLD. The APM Seal will provide users, rights holders, etc., with a direct link to an Abuse Prevention and Mitigation Reporting Website (“APM Reporting Website”), which contains a clear description and instructions that will provide the inquiring party with guidance on how to report infringement or other abusive conduct, including but not limited to the conduct identified in response to Question 28 to the Registry and relevant authorities. This will allow the user a direct and practical means of pursuing any complaints it may have.

The Applicant will implement a Governance Council, which will lead the policy development process of defining how the APM Reporting Website should best reflect the options users, rights holders, etc., have for addressing infringing content or other issues.

The APM Seal will operate as follows:

a)The Registrant will be required to agree to the Applicant′s AUP as part of the Registration process for the second-level domains.
b)The Terms and Conditions will require the Registrant to include the APM Seal in a prominent place on its website.

c)Following the registration, the Registry will automatically email the Registrant’s Administrative, Technical, and Billing contacts with an additional notification that the APM Seal needs to be included on the Registrant’s homepage. The Registrant has 120 days from the date of registration (the “Grace Period”) to effectuate the fixing of the APM seal.
d)During the Grace Period, the domain registration will be flagged in WHOIS or a linked system as being in the APM Seal Grace Period.
e)When the APM Seal has been activated, the second-level domain will have the APM Seal marked as active in WHOIS or a linked system.
f)If the Registrant does not activate the APM Seal before the Grace Period expires, the domain name will be flagged as being out of the Grace Period for the APM Seal activation and the Registry will notify the Registrant’s Administrative, Technical, and Billing contacts that this APM Seal activation is out of its Grace Period. The Registrant has an additional 30 days to include the APM Seal on the homepage or the site is flagged as in breach of the Registration terms.
g)Should the registrant fail to comply and activate the APM Seal within the period specified in the AUP, the Registry will conduct an investigation on that domain. If after the investigation it is determined that the domain is in breach of the AUP the Registry reserves the right to suspend and cancel the domain.
h)Exceptions include, but are not limited to situations where a Registrar has a second-level domain that is:

(a) Used for forwarding to another domain,
(b) Not used for a website,
(c) Currently not in use, or
(d) There is another reason why the seal cannot technically be included

If a site is listed to be in any of these exception states and then the use of the domain changes to a state that would require the APM Seal, the Registrant must then change the domain’s status to comply with the AUP. The Registry will conduct an investigation to ensure compliance with the policy upon notification that a site is out of compliance via the Rights Contact. If after the investigation it is determined that the domain is in breach of the AUP the Registry reserves the right to suspend and cancel the domain.

5 Efforts to promote WHOIS Accuracy

5.1. Thick WHOIS
The Applicant will include a thick searchable WHOIS database both accessible on port 43 as well as on port 80 (http) as required in Specification 4 of the Registry Agreement. A thick WHOIS provides numerous advantages including a centralized location of registrant information, the ability to more easily manage and control the accuracy of data, and a consistent user experience, as well as greater transparency, a factor critical to rights holders as well as law enforcement in pursuing abusive uses of a domain.

5.2. Bi-Annual Audits to Ensure Accurate WHOIS
The Applicant’s TVT will perform a bi-annual review of a random sampling of domain names within the applied-for gTLD to test the accuracy and authenticity of the WHOIS information. Through this review, the Applicant’s TVT will examine the WHOIS data for evidence of inaccurate or incomplete Whois information. In the event that such errors or missing information exists, it shall be forwarded to the Registrar, who shall be required to address such deficiencies with its Registrants.

6 Policies Handling Complaints Regarding Abuse and Rights Issues
In addition to the RPMs addressed above, the Applicant will implement a number of measures to handle complaints regarding the abusive registration of domain names in its gTLD that may infringe on the rights of others. Further details are described in

the response to Question 28.

7 Registry Acceptable Use Policy
One of the key policies each new gTLD Registry needs is to have an AUP that clearly delineates the types of activities that constitute “abuse” and the repercussions associated with an abusive domain name registration. The policy must be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the Registry to take the appropriate actions based on the type of abuse. This may include locking down the domain name preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name “on hold” rendering the domain name non-resolvable, transferring the domain name to another Registrar, and⁄or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation. The gTLD’s AUP, set forth in our response to Question 28, will include prohibitions on phishing, pharming, dissemination of malware, fast flux hosting, hacking, and child pornography. In addition, the policy will include the right of the Registry to take action necessary to deny, cancel, suspend, lock, or transfer any registration in violation of the policy.
In addition, the Applicant reserves the right to deny attempted registrations from repeat violators of the Registry’s AUP. The Registry’s AUP will incorporate a certification by the registrant that the domain will be used only for licensed, legitimate activities, and not to facilitate piracy or infringements. The registrant will be required to accept these terms as part of its registration agreement. The Applicant reserves the right to suspend or cancel a domain for violation of the Registry’s AUP.

8 Monitoring for Malicious Activity
The Applicant is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the AUP are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or are part of a real-time investigation by law enforcement.
Once a complaint is received or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring Registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or to provide a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on “ServerHold”. Although this action removes the domain name from the gTLD zone, the domain name record still appears in the gTLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

9 Resourcing Plans Specific to Backend Registry Activities
Responsibility for rights protection rests with a variety of functional groups. The Trademark Validation Team and Sunrise Validation Teams are primarily responsible for investigating claims of marks for domain registration. The customer service team also plays an important role in assisting with the investigations, responding to customers, and notifying Registrars of abusive domains. Finally, the Policy⁄Legal team is responsible for developing the relevant policies and procedures.

The rights protection mechanisms described in the response above involve a wide range of tasks, procedures, and systems. The responsibility for each mechanism varies based on the specific requirements. In general the development of applications such as sunrise and IP claims is the responsibility of the Engineering team, with guidance from the Product Management team. Customer Support and Legal play a critical role in

enforcing certain policies such as the rapid suspension process. These teams have very substantial experience implementing these or similar processes.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources will be made available:
-Development⁄Engineering – 19 people
-Product Management - 4 people
-Customer Support – 12 people
The resources are more than adequate to support the rights protection mechanisms of the Registry.

Administrative Services Provider – Famous Four Media Limited

In addition to those resources set out above provided by the Registry's backend services provider the Applicant's Administration Services Provider shall provide the following extra resources:
-Sunrise Validation Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
-Ongoing Rights Protection Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
The two key objectives of the Sunrise Validation Team and the Ongoing rights Protection Team (together the "Rights Team") is to:

a)Prevent abusive registrations; and
b)Identify and address the abusive use of registered names on an ongoing basis
Given that rights protection is a fundamental core objective of the Applicant it has contracted with its Registry Administration Services Provider that the number of full time personnel made available to the Applicant will be 125% of the estimated requirement to ensure that at all times the Applicant is over resourced in this area. In addition the Applicant shall instruct outside Counsel in any relevant jurisdiction on all matters that are unable to be adequately dealt with by the Sunrise Validation Team or the Ongoing Rights Protection Team.

10 Registry Backend Services Provider Experience with Rights Protection Measures
The gTLD's Registry Backend Services Provider, Neustar Inc., has already implemented Sunrise and⁄or Trademark Claims programs for numerous gTLDs including .biz, .us, .travel, .tel and .co and will implement both of these services on behalf of the Applicant.

Neustar's Experience with Sunrise Process:
In early 2002, Neustar became the first Registry operator to successfully launch an authenticated Sunrise process. This process permitted qualified trademark owners to pre-register their trademarks as domain names in the .us gTLD space prior to the opening of the space to the general public. Unlike any other "Sunrise" plans implemented or proposed before that time, Neustar validated the authenticity of trademark applications and registrations with the United States Patent and Trademark Office (USPTO).
As the back-end Registry operator for the .tel gTLD and the .co ccTLD, Neustar launched a validated Sunrise program employing processes that are very similar to those that will be used by the TMCH for new gTLDs.
Below is a high level overview of the implementation of the .co Sunrise period and the Trademark Claims service that was part of the .biz launch. Neustar's experience in each of these RPMs will enable it to seamlessly provide these services on behalf of the Applicant as required by ICANN.
Sunrise and .co
The Sunrise process for .co was divided into two sub-phases:
- Local Sunrise giving holders of eligible trademarks that have obtained registered status from the Colombian trademark office the opportunity to apply for the .co domain

names corresponding with their marks.
- Global Sunrise program giving holders of eligible registered trademarks of national effect, that have obtained a registered status in any country of the world the opportunity to apply for.co domain names corresponding with their marks for a period of time before registration is open to the public at large.

Like the new gTLD process set forth in the Applicant Guidebook, trademark owners had to have their rights validated by a Clearinghouse provider prior to the registration being accepted by the Registry. The Clearinghouse used a defined process for checking the eligibility of the legal rights claimed as the basis of each Sunrise application using official national trademark databases and submitted documentary evidence.

Applicants and⁄or their designated agents had the option of interacting directly with the Clearinghouse to ensure their applications were accurate and complete prior to submitting them to the Registry via an optional "Pre-validation Process". Regardless of whether an Applicant was "pre-validated", all Applicants had to submit their corresponding domain name applications through a .co accredited Registrar. When the Applicant was pre-validated through the Clearinghouse, they were given an associated approval number that had to be supplied to the Registry. If Applicants were not pre-validated, they were required to submit the necessary trademark information through their Registrar to the Registry.

At the Registry level, Neustar, subsequently either delivered the:
- Approval number and domain name registration information to the Clearinghouse, or
- When there was no approval number, trademark information and the domain name registration information was provided to the Clearinghouse through EPP (as is currently required under the Applicant Guidebook).

Information was then used by the Clearinghouse for further validation of those pre-validated applications, or initial validation of those that did not select pre-validation. If the Applicant was validated and their trademark matched the domain name applied for, the Clearinghouse communicated that fact to the Registry via EPP.

When there was only one validated sunrise application for a domain name, the application proceeded to registration when the .co launched. If there were multiple validated applications for the same domain name (recognizing that there could be multiple trademark owners sharing the same trademark), those were processed via the .co Sunrise auction process. Neustar tracked all of the information it received and the status of each application on a secure Website to enable trademark owners to view the status of their Sunrise application.

Although the exact process for the Sunrise program and its interaction with trademark owners, Registry, Registrars, and TMCH is not finalized at the time of the application, Neustar's expertise in launching multiple Sunrise processes and its established software will ensure a smooth and compliant Sunrise process for the new gTLDs.

a) Trademark Claims Service Experience

When Neustar's .biz gTLD launched in 2001, Neustar became the first gTLD with a Trademark Claims ("TC") service. Neustar developed the TC Service by enabling companies to stake claims to domain names prior to the commencement of live .biz domain registrations.

During the TC process, Neustar received over 80,000 TC from entities around the world. Recognizing that multiple intellectual property owners could have trademark rights in a particular mark, multiple TC for the same string were accepted. All applications were logged into a TC database managed by Neustar.

The Trademark Claimant was required to provide various information about their trademark rights, including the:
- Particular trademark or service mark relied on for the trademark Claim
- Date a trademark application on the mark was filed, if any, on the string of the domain name
- Country where the mark was filed, if applicable
- Registration date, if applicable
- Class or classes of goods and services for which the trademark or service mark was registered

- Name of a contact person with whom to discuss the claimed trademark rights.

Once all TC and domain name applications were collected, Neustar then compared the claims contained within the TC database with its database of collected domain name applications (DNAs). In the event of a match between a TC and a domain name application, an e-mail message was sent to the domain name Applicant notifying the Applicant of the existing TC. The e-mail also stressed that if the Applicant chose to continue the application process and was ultimately selected as the registrant, the Applicant would be subject to Neustar's dispute proceedings if challenged by the Trademark Claimant for that particular domain name.

The domain name Applicant had the option to proceed with the application or cancel the application. Proceeding with an application meant that the Applicant wanted the application to proceed to registration despite having been notified of an existing Trademark Claim. By choosing to "cancel," the Applicant made a decision in light of an existing TC notification to not proceed.

If the Applicant did not respond to the e-mail notification from Neustar, or elected to cancel the application, the application was not processed. This prevented the Applicant from registering the actual domain name. If the Applicant affirmatively elected to continue the application process after being notified of the claimant's (or claimants') alleged trademark rights to the desired domain name, Neustar processed the application.

This process is very similar to the one ultimately adopted by ICANN and incorporated in the latest version of the Applicant Guidebook. Although the collection of TC for new gTLDs will be by the TMCH, many of the aspects of Neustar's TC process in 2001 are similar to those in the Applicant Guidebook. This makes Neustar uniquely qualified to implement the new gTLD TC process.

Neustar was also a key contributor to the development of the Uniform Dispute Resolution Policy ("UDRP") in 1998. This became the first "Consensus Policy" of ICANN and has been required to be implemented by all domain name registries since that time. The UDRP is intended to be an alternative dispute resolution process to transfer domain names from those that have registered and used domain names in bad faith. Although there is not much of an active role that the domain name Registry plays in the implementation of the UDRP, Neustar has closely monitored UDRP decisions that have involved the gTLDs which it supports and ensures that the decisions are implemented by the Registrars supporting its gTLDs.

-end-

30(a). Security Policy: Summary of the security policy for the proposed registry

Q30A

The Applicant and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The Applicant's registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

The Applicant and Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.

The following is a summary of the security policies that will be used in the Applicant's registry, including:

1. Summary of the security policies used in the registry operations

2. Description of independent security assessments
3. Description of security features that are appropriate for the TLD
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the Applicant’s registry.

30(a).1 Summary of Security Policies
Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar’s obligations under applicable law, regulations, and contracts. This Program establishes Neustar’s policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.

The Program defines:
- The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.
- The rights that can be expected with that use.
- The standards that must be met to effectively comply with policy.
- The responsibilities of the owners, maintainers, and users of Neustar’s information resources.
- Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy
The Acceptable Use Policy provides the “rules of behavior” covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy
The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy
The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy
The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy
The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy
The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting

“lessons learned” post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy
The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy
Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy
The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system⁄application accounts, shared⁄group accounts, guest⁄public accounts, temporary⁄emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy
The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy
The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy
The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy
The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy
The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy
The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.

30.(a).2 Independent Assessment Reports
Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.

External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

- A network survey is performed in order to gain a better knowledge of the network that was being tested
- Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase
- Identification of key systems for further exploitation is conducted
- Exploitation of the identified systems is attempted.

Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management's prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.

30.(a).3 Augmented Security Levels and Capabilities
The Applicant and its backend provider Neustar will provide the same high level of security provided across all of the registries it manages.

A key to Neustar's Operational success is Neustar's highly structured operations practices. The standards and governance of these processes:
- Include annual independent review of information security practices
- Include annual external penetration tests by a third party
- Conform to the ISO 9001 standard (Part of Neustar's ISO-based Quality Management System)
- Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices
- Are aligned with all aspects of ISO IEC 17799
- Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)
- Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4 below.

BITS Recommendations
The Applicant will structure its policies around the BITS Recommendations where relevant to this gTLD.

The Applicants goal with this gTLD is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the TLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial TLDs. The policy comprises of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial TLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http:⁄⁄www.icann.org⁄en⁄correspondence⁄aba-bits-to-beckstrom-crocker-20dec11-en.pdf]

We welcome the recommendations from SSWG and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.
Coalition for Online Accountability (“COA”) Recommendations

The Applicant will structure its policies around the COA Recommendations where relevant to this gTLD.

The Applicant’s goal with this gTLD is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD’s reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy comprises of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http:⁄⁄bit.ly⁄HuHtmq.

We welcome the recommendations from the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

30.(a).4 Commitments and Security Levels
The Applicant’s registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:

Compliance with High Security Standards
- Security procedures and practices that are in alignment with ISO 17799
- Annual SOC 2 Audits on all critical registry systems
- Annual 3rd Party Penetration Tests
- Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies
- Compliance with all provisions described in section 30.(a).4 below and in the attached security policy document.
- Resources necessary for providing information security
- Fully documented security policies
- Annual security training for all operations personnel

High Levels of Registry Security
- Multiple redundant data centers
- High Availability Design
- Architecture that includes multiple layers of security

- Diversified firewall and networking hardware vendors
- Multi-factor authentication for accessing registry systems
- Physical security access controls
- A 24x7 manned Network Operations Center that monitors all systems and applications
- A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks
- DDoS mitigation using traffic scrubbing technologies

We commit to the following:

– Safeguarding the confidentiality, integrity and availability of registrant’s data.
– Compliance with the relevant regulation and legislation with respect to privacy.
– Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
– Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
– That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.
– That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
– A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
– Those emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

The Applicant will further be implementing a thorough and extensive Abuse Prevention and Mitigation plan, designed to minimise abusive registrations and other detrimental activities that may impact security and negatively impact internet users. This plan includes the establishment of 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 gTLD through all Registrars of record, including those involving a reseller. Details of this point of contact will be clearly published on the Applicant’s website.

The following is an overview of certain other security related initiatives undertaken by the Applicant - (see response to Q28 for more detail):

- Policies and Procedures to Minimize Abusive Registrations
- Abuse Point of Contact
- Policies for Handling Complaints Regarding the Abuse Policy
- Acceptable Use Policy (”AUP”)
- Measures for removal of Orphan Glue records
- Measures to promote Whois accuracy both directly by the Registry and by Registrars via requirements in the Registry-Registrar Agreement (“RRA”)):
    - Registry semi-annual WHOIS verification
    - Authentication of Registrant information as complete and accurate at time of registration.
    - Regular monitoring of registration data for accuracy and completeness
    - Registrar self-certification
    - WHOIS Data reminder processes
    - Establishing policies and procedures to ensure Registrar compliance with policies, which may include audits, financial incentives, penalties, or other means.
    - Registrar verification of WHOIS
- Policies and procedures that define malicious or abusive behavior
- Abuse Response Process
    - Service Levels Requirements for Resolution
    - Service Levels Requirements for Law enforcement Requests

- Coordination with Industry Groups and Law Enforcement
- Controls to ensure proper access to domain functions:
  - Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests;
  - Enabling multiple, unique points of contact to request and⁄or approve update, transfer, and deletion requests;
  - Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted
- Additional Abuse Prevention and Mitigation initiatives:
  - Additional Mechanism for Protection of Capital City Names
  - Additional Mechanisms to Protect and Reserve IGO Names
- Increasing Registrant Security Awareness
- Registrant Disqualification
- Restrictions on Proxy Registration Services
- Registry Lock Option

Resourcing Plans

The development and maintenance of the information security policies and practices are the primary responsibility of the Information Security team. As described in response to Question 31, the information security team is comprised of highly trained security professionals. They establish security policies, actively monitor for intrusions and other nefarious activity, and ensure that all Neustar employees are adhering to Neustar's security policies and best practices. These engineers ensure that the registry data is not compromised in any way.
The necessary resources to support all of the registry's security needs will be pulled from the pool of resources described in detail in the response to Question 31. The following resources are available from the team:

- Information Security - 16 employees

The resources are more than adequate to support the database needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

© Internet Corporation For Assigned Names and Numbers.