# Appendix A

## Community Objection Upheld  Against Amazon's Application for .MOBILE Due to Exclusice Access Policies

**THE INTERNATIONAL CENTRE FOR EXPERTISE OF THE**

**INTERNATIONAL CHAMBER OF COMMERCE**

CASE No. EXP/499/ICANN/116

CTIA – THE WIRELESS ASSOCIATION® (USA)

vs/

AMAZON EU S.À R.L. (LUXEMBOURG)

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.

**THE INTERNATIONAL CENTRE FOR EXPERTISE OF THE INTERNATIONAL CHAMBER OF COMMERCE**

**CASE No. EXP/499/ICANN/116**

In the matter of an objection under the
ICANN New Generic Top-Level Domain Dispute Resolution Procedure

*Between*

| | |
|---|---|
| **CTIA – The Wireless Association ® (USA)** | **OBJECTOR** |

*and*

| | |
|---|---|
| **Amazon EU S.à r.l. (Luxembourg)** | **APPLICANT / RESPONDENT** |

# Expert Determination

**Expert Panel:**

Kap-You (Kevin) Kim

# TABLE OF CONTENTS

## 1. INTRODUCTION

1. Under the Internet Corporation for Assigned Names and Numbers (*"**ICANN**"*) new generic Top-Level Domain (*"**gTLD**"*) name program (*"**Program**"*), the Applicant (Amazon EU S.à r.l.) has submitted an application (*"**Application**"*) for the string **<.MOBILE>**.[1] The Objector (CTIA – The Wireless Association) has filed an objection (*"**Objection**"*) pursuant to the applicable rules, and the Applicant has filed a response (*"**Response**"*).

2. This Expert Determination is a decision upon the merits of the Objection. For the reasons explained below, I have determined that Objector has satisfied all the requirements for a Community Objection. The Objection is upheld.

## 2. PRELIMINARIES

### 2.1. The Parties

3. The Objector is CTIA – The Wireless Association® Contact Information Redacted Contact Information Redacted

4. The Objector is represented by Ms. Kathryn A. Kleiman and Mr. Robert J. Butler, FLETCHER, HEALD & HILDRETH, PLC Contact Information Redacted Contact Information Redacted

5. The Applicant is Amazon EU S.à r.l. Contact Information Redacted

6. The Applicant is represented by Mr. Douglas M. Isenberg, THE GIGALAW FIRM Contact Information R Contact Information Redacted Contact Information Redacted

### 2.2. The Expert Panel

7. The Expert Panel comprises a sole Expert, Mr. Kap-you (Kevin) Kim, BAE, KIM & LEE LLC Contact Information Redacted

[1] The Application can be found online at: https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/969.

### 2.3. The New gTLD String Objected To

8. The new gTLD string applied for and objected to is: **.MOBILE**

### 2.4. Nature of the Objection

9. Section 2(e) of the Procedure provides for four categories of permissible objections:

> *The grounds upon which an objection to a new gTLD may be filed are set out in full in Module 3 of the Applicant Guidebook. Such grounds are identified in this Procedure, and are based upon the Final Report on the Introduction of New Generic Top-Level Domains, dated 7 August 2007, issued by the ICANN Generic Names Supporting Organization (GNSO), as follows:*
>
> *(i) "String Confusion Objection" refers to the objection that the string comprising the potential gTLD is confusingly similar to an existing top-level domain or another string applied for in the same round of applications.*
>
> *(ii) "Existing Legal Rights Objection" refers to the objection that the string comprising the potential new gTLD infringes the existing legal rights of others that are recognized or enforceable under generally accepted and internationally recognized principles of law.*
>
> *(iii) "Limited Public Interest Objection" refers to the objection that the string comprising the potential new gTLD is contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law.*
>
> *(iv) "Community Objection" refers to the objection that there is substantial opposition to the application from a significant portion of the community to which the string may be explicitly or implicitly targeted.*

10. In this case, the Objection is a "Community Objection."

### 2.5. Applicable Rules

11. The Program provides a process for the introduction of new gTLDs in the internet, such as the .MOBILE string at issue in this proceeding. The procedures of the Program are detailed in the gTLD Applicant Guidebook ("***Guidebook***").[2] The Guidebook provides substantive and procedural criteria, standards and rules related to virtually every aspect of the gTLD application, evaluation, objection and dispute resolution process.

12. Module 3 of the Guidebook, entitled "Objection Procedures", and the Attachment to

[2] I refer to and rely on version 2012-06-04 of the Guidebook, dated 4 June 2012.

Module 3, entitled "New gTLD Dispute Resolution Procedure" ("***Procedure***"), are particularly relevant to these proceedings. Module 3 describes *"the guiding principles, or standards, that each dispute resolution panel will apply in reaching its expert determination."*[3] The Procedure details procedures for resolving new gTLD disputes.

13. In addition, the ICC Expertise Rules (*"**ICC Rules**"*) of the International Centre for Expertise (*"**Centre**"*) of the International Chamber of Commerce (*"**ICC**"*) supplemented by the ICC Practice Note on the Administration of Cases under the Procedure also apply to these proceedings.

14. Collectively, the above are *"**the Rules**."*

### 2.6. Standard and Burden of Proof

15. In deciding on an objection, the expert shall apply the standards that have been defined by ICANN.[4] Section 3.5 of Module 3 of the Guidebook on "Dispute Resolution Principles (Standards)" lays down the procedure for each of the four types of objections under the Rules. Section 3.5.4 of Module 3 of the Guidebook contains the standards applicable to Community Objections. In addition, the expert may rely upon the statements and documents submitted by the parties and any rules or principles that he finds to be applicable.[5]

16. As per the Rules, the burden of establishing that the Objection should be sustained lies upon the Objector.[6]

### 2.7. Miscellaneous

17. The language of these proceedings is English.[7] All written materials and communications among the parties and the Expert Panel have been in English.[8]

18. All submissions and communications were exchanged between the parties and the

[3] Guidebook (Module 3), introduction.

[4] Procedure, Article 20(a).

[5] Id., Article 20(b).

[6] Id., Article 20(c).

[7] Procedure, Article 5(a).

[8] Procedure, Article 6(a).

Panel electronically, copying the Centre (the appointed Dispute Resolution Service Provider or "***DSRP***").[9]

19. The place of the proceedings is Paris, France, where the DRSP (i.e., the Centre) is located.[10]

## 3. PROCEDURAL BACKGROUND

20. The Application was submitted on 13 June 2012.

21. The Objection was submitted on 13 March 2013.

22. The Centre conducted an administrative review of the Objection and issued a notice dated 5 April 2013 indicating that the Objection was in compliance with the Procedure and the ICC Rules.

23. On 12 April 2013, ICANN published a list of all Objections which passed the DRSP's Administrative reviews (ICANN Dispute Resolution Announcement). And in a letter dated 19 April 2013, the Centre invited the Applicant to submit a Response under Article 11(b) of the Procedure.

24. In a letter dated 12 April 2013, the Centre notified the parties that it was considering consolidating this case with another case involving an objection submitted by the Objector related to the .MOBILE string application by Dish DBS Corporation (EXP/498/ICANN/115) and invited the parties to comment on this. After receipt of the parties' comments, the Centre issued its decision not to consolidate the two cases on 19 April 2013. The question of consolidation was revived at the request of the applicant in EXP/498/ICANN/115. On 3 May 2013, after receipt of parties' comments, the Centre again decided against consolidation.

25. The Centre conducted an administrative review of the Response and issued a notice dated 27 May 2013 indicating that the Response was in compliance with the Procedure and the ICC Rules.

[9] Procedure, Article 6(b).

[10] Procedure, Article 4(d).

26. The Chair of the Standing Committee of the Centre appointed the Expert on 14 June 2013, and the parties were informed of this by letter from the Centre dated 21 June 2013.

27. On 24 July 2013, the Centre confirmed that the parties had paid the estimated costs, confirmed the full constitution of the Expert Panel and transferred the file to me.

28. The parties then jointly requested a series of procedural stays on the reported ground that the .MOBILE New gTLD application that is the subject of this proceeding might be determined to fall within the ICANN Board's definition of a "Generic String" application with exclusive registry access, and that this might impact the nature and outcome of these proceedings. The stay requests were as follows:

(1) On or around 29 July 2013, the parties jointly requested a 30-day stay of the proceedings, which I granted on the same day.

(2) On or around 28 August 2013, the parties jointly requested a second stay, of 40 days, which I granted on 30 August 2013.

(3) On or around 9 October 2013, the parties jointly requested a third stay, of 15 days, which I granted on 10 October 2013 and confirmed on 15 October 2013.

(4) On or around 23 October 2013, the parties jointly requested a fourth stay, of 60 days, which I granted on 24 October 2013.

(5) Then, on or around 23 December 2013, the Objector submitted a document purporting to be a joint request for an additional stay of 60 days. However, Applicant objected to the additional stay. As the Rules do not provide for the Expert to unilaterally stay the proceedings without the agreement of all parties, no stay was granted.

29. During this period of repeated stay requests, ICANN and various interested parties discussed the issue of closed generic gTLDs. As noted in the Objector's latest stay request in late December 2013, the ICANN Governmental Advisory Committee (GAC) issued advice to the ICANN Board of Directors regarding New gTLD applications in a

so-called "Beijing Communiqué."[11] Among other things, the GAC addressed strings that represent "generic terms" and the issue of exclusive access. The GAC stated (in Annex 1 "Safeguards on New gTLDs," under "Category 2) that "[f]or strings representing generic terms, exclusive registry access should serve a public interest goal." It then identified a "non-exhaustive list of strings that it considers to be generic terms, where the applicant is currently proposing to provide exclusive registry access." Among them was the .MOBILE string.

30. In response, ICANN invited Applicants who had applied for the gTLDs so identified by the GAC to respond and clarify whether they still intended to operate the new gTLD as an "exclusive access registry."

31. In an official "Response Form for Applicants" in connection with "GAC Advice Category 2: Exclusive Access," which has been publicly posted, Amazon responded:

(1) "**No**" to the question "**Will the TLD be operated as an exclusive access registry?**";

(2) "**Yes**" to the question "**Does your current application state that the TLD will be operated as an exclusive registry?**"; and

(3) "**No**" to the question "**Do you have a pending change request regarding exclusive access?**"[12]

32. In response to Applicant's objection to a further stay, Objector complained in an email dated 23 December 2013 that given the above development relating to whether .MOBILE would be a closed or open registry, the matter should be stayed pending amendment of the Application. Applicant responded in an email dated 24 December 2013 that Objector's email dated 23 December 2013 had addressed "substantive issues" and should be ignored or, absent that, Applicant should be given an opportunity to respond. Objector then responded by email dated 25 December 2013 that it "fully support[ed] Applicant's request to file an additional submission."

[11] The GAC's "Beijing Communique" can be found online here: http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf.

[12] Amazon's response can be found online here: http://newgtlds.icann.org/sites/default/files/applicants/09oct13/gac-advice-response-1-1316-6133-en.pdf.

Applicant in turn (by email dated 26 December 2013) clarified that it was not making such a request. I then solicited clarification from the Applicant in an email dated 4 January 2014:

> *I understand that the Objector has requested a further stay and that the Applicant does not concur. Before proceeding, the Tribunal invites the Applicant to clarify its position by no later than Friday, 10 January regarding to whether .MOBILE will be operated as a closed or exclusive access registry and whether Amazon has or intends to amend its Closed Generic application relating to this question.*

33. Applicant responded in an email dated 8 January 2014:

> *Amazon will not operate .MOBILE as an "exclusive access registry," and Amazon intends to amend its application to reflect this prior to entering into a Registry Agreement, as required by ICANN. For reference, please see ICANN's notice dated October 9, 2013, regarding recent GAC advice and ICANN's new limitations on "exclusive access registries" (available at http://newgtlds.icann.org/en/announcements-and-media/announcement-4-09oct13-en) as well as Amazon's public response to ICANN (PDF attached, also available at http://newgtlds.icann.org/en/applicants/gac-advice/cat2-safeguards).*

34. Objector responded in an email dated 11 January 2014:

> *In view of Applicant's confirmation below that its application as currently on file and before this Tribunal is not a true and accurate representation of Applicant's business plans with respect to the .MOBILE gTLD, Objector CTIA maintains its request for a stay of this proceeding until such time as Applicant amends its application to correct the inaccuracies and describes in reviewable detail its plans for operation of .MOBILE as a non-exclusive access registry. A stay is warranted in order to preserve Objector's rights to review, object to, and receive a Panel decision on the actual application and to preserve the integrity of the Panel's and Tribunal's decision-making processes.*

35. Following this, I requested further clarification from Applicant in an email dated 24 January 2014:

> *I understand that Applicant (1) acknowledges that its current application on file states that it intends to operate the .MOBILE as an "exclusive access registry," (2) has expressed the intention to amend its application to reflect an intention not to operate the .MOBILE as an "exclusive access registry" prior to entering into a Registry Agreement, but (3) has not yet amended its application to reflect this intention. [...]*
>
> *I have no reason to question Applicant's intentions. However, I am not certain that independent assurances by Applicant are a proper foundation on which to render a decision. Therefore, before deciding whether or not to stay this matter, I would ask Applicant whether it accepts to have a decision rendered based on its*

> *application which currently expresses an intention to operate the .MOBILE as an "exclusive access registry"; or, if not, to provide reasons why it believes that a decision may be rendered based on the declaration of intentions reflected in the response form found at the url link above, without amending the application itself.*

36. Applicant then responded in an email dated 27 January 2014, stating, *inter alia*:

> *Applicant believes that the decision in this proceeding should be based on the Objection filed by the Objector on March 13, 2013, and the Response filed by the Applicant on May 16, 2013 – each of which relates to Application ID 1-1316-6133, a copy of which was posted by ICANN on June 13, 2012* [...].

I inferred from this that Applicant did not consider that a further stay, further briefing or a hearing was required, but rather held the view that a decision should be rendered forthwith based on the contents of the Objection and Response.

37. On 29 January 2014, Objector responded, stating, *inter alia*:

> [A]*n application for a New gTLD must be "true and accurate and complete in all material respects." See Module 6, Section 1, Applicant Guidebook. Applicant admits that its Application does not satisfy these fundamental criteria for proceeding with its evaluation. A mere statement of intent to amend does not render the Application true or complete, nor does it permit a substantive review of the actual application as it will ultimately exist. Accordingly, the Panel cannot accept Applicant's representation of non-exclusivity and simply proceed to decision at this time. Rather, the Panel and Objector need to see the details of the promised amendment, and Objector must be given an opportunity to review and comment to preserve our rights as representatives of the Mobile Wireless Community.*
>
> [...]
>
> *Importantly, it is not acceptable under any concept of ICANN principles, due process or public equity and fairness to allow Applicant to proceed on its fictional application and then, even if the Objection is sustained, argue that it can still amend and proceed with an amended application while wholly circumventing the necessary and authorized community review of that actual amended application through the Objection Process. Any such attempt to "game the system" should be summarily rejected.*

38. In sum, although Applicant has stated an intention to revise the Application to provide for an open registry, it insists that I issue my Expert Determination without any further stay to allow it to revise its Application accordingly. Given that the Program is intended to allow objections to be lodged in response to submitted applications, it would be inappropriate to make a determination based on a hypothetical application. Therefore, in light of the Rules and the foregoing exchange, I issue this Expert Determination based on the contents of the Objection and the Response, which

address the unrevised Application, and without regard to any hypothetical revision of the Application which might provide for an open registry for the .MOBILE gTLD string.

39. On 3 March 2014, having considered the parties' respective comments and the relevant provisions of the Rules, I informed the parties by email of my decision not to stay the proceedings and that I would endeavor to issue the Expert Determination expeditiously.

40. I have decided that there is no need for additional written submissions from the parties beyond the Objection, the Response and the submissions I had solicited from the parties in the communications set out above between late December and the end of January.[13]

41. In addition, I note that neither party has requested a hearing. Bearing in mind the parties' stated positions above and the overall circumstances, and in light of the preference against hearings in the Procedure,[14] I have decided there is no need to convene a hearing.

42. I sent the draft Expert Determination to the Centre for its review on 18 March 2013. Although Article 21(1) of the Procedure stipulates that "the DRSP and the Panel shall make reasonable efforts to ensure that the Expert Determination is rendered within forty-five (45) days of the constitution of the Panel," this was not possible in view of the parties' joint stays and dispute regarding an additional stay requested by the Objector. Nonetheless, the Expert Determination has been issued within 45 days of my decision not to further stay the proceedings issued on 3 March 2014.

## 4. REQUIREMENTS

### 4.1. Standing Requirements

43. Section 3.2.2.4 of the Guidebook explains who has standing to submit a Community

[13] See Procedure, Article 17.

[14] See Procedure, Article 19(a)-(b):

> *(a) Disputes under this Procedure and the applicable DRSP Rules will usually be resolved without a hearing.*
> *(b) The Panel may decide, on its own initiative or at the request of a party, to hold a hearing only in extraordinary circumstances.*

Objection, stating:

> *Established institutions associated with clearly delineated communities are eligible to file a community objection. The community named by the objector must be a community strongly associated with the applied-for gTLD string in the application that is the subject of the objection.*
>
> *To qualify for standing for a community objection, the objector must prove both of the following:*
>
> ***It is an established institution** – Factors that may be considered in making this determination include, but are not limited to:*
>
> - *Level of global recognition of the institution;*
> - *Length of time the institution has been in existence; and*
> - *Public historical evidence of its existence, such as the presence of a formal charter or national or international registration, or validation by a government, inter-governmental organization, or treaty. The institution must not have been established solely in conjunction with the gTLD application process.*
>
> ***It has an ongoing relationship with a clearly delineated community** – Factors that may be considered in making this determination include, but are not limited to:*
>
> - *The presence of mechanisms for participation in activities, membership, and leadership;*
> - *Institutional purpose related to the benefit of the associated community;*
> - *Performance of regular activities that benefit the associated community; and*
> - *The level of formal boundaries around the community.*

44. The article concludes by stating that the expert's task is to "perform a balancing of the factors listed above, as well as other relevant information, in making its determination" and "[i]t is not expected that an objector must demonstrate satisfaction of each and every factor considered in order to satisfy the standing requirements."

45. Although the rule seems to present two mandatory tests for standing, in fact there are three, since the first paragraph also dictates that "[t]he community named by the objector must be a community strongly associated with the applied-for gTLD string in the application that is the subject of the objection."

46. In sum, the standing tests require the would-be objector to demonstrate that it is (1) an "established institution", (2) with an "ongoing relationship with a clearly delineated community", and further, (3) that the named community is "strongly associated with the applied-for gTLD string."

### 4.2. Merits Requirements for a Community Objection

47. Should the Objector meet the requirements for standing, to be successful on its Objection, it must then meet the substantive requirements for a Community Objection set out in section 3.5.4 of Module 3 of the Guidebook, which reads:

> *The four tests described here will enable a DRSP panel to determine whether there is substantial opposition from a significant portion of the community to which the string may be targeted. For an objection to be successful, the objector must prove that:*
>
> *•The community invoked by the objector is a clearly delineated community; and*
>
> *•Community opposition to the application is substantial; and*
>
> *•There is a strong association between the community invoked and the applied-for gTLD string; and*
>
> *•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. Each of these tests is described in further detail below.*

48. The four tests are eliminatory; that is, if any one of them is not satisfied, the Objection must be denied. Each element is further broken down according to factors that may be considered by the Expert in deciding whether that particular element has been satisfied. These factors will be considered in the context of the relevant analysis below.

### 4.3. Issues Common to Both Standing and Merits: the "Community Test"

49. Both the standing and merits tests require proof of a "clearly delineated community" and a "strong association" between the invoked community and the applied-for gTLD string. I consider these common connections in the following subsections.

#### *4.3.1. "Clearly Delineated Community"*

50. As mentioned above, the Guidebook lists the following non-exclusive and non-mandatory "factors that may be considered" in determining whether the objector has an "ongoing relationship with a clearly delineated community" for purposes of standing:

> - *The presence of mechanisms for participation in activities, membership, and leadership;*
> - *Institutional purpose related to the benefit of the associated community;*
> - *Performance of regular activities that benefit the associated community; and*

- *The level of formal boundaries around the community.*[15]

Among the listed factors, the last one appears to be the most logically connected to the "clearly delineated community" aspect of the requirement.

51. This same factor is also folded into the more extensive list suggested for consideration under the merits tests, for which the Guidebook suggests that the Expert Panel "could balance a number of factors ... including but not limited to the following":

    - *The level of public recognition of the group as a community at a local and/or global level;*
    - *The level of formal boundaries around the community and what persons or entities are considered to form the community;*
    - *The length of time the community has been in existence;*
    - *The global distribution of the community (this may not apply if the community is territorial); and*
    - *The number of people or entities that make up the community.*[16]

52. The rule emphasizes the mandatory nature of this community requirement: "If opposition by a number of people/entities is found, but the group represented by the objector is not determined to be a clearly delineated community, the objection will fail."[17] In other words, irrespective of the number involved or the strength of their opposition, only a clearly delineated community's objections will be recognized.

53. Although the merits test provides a more elaborate analytical framework and perhaps a stricter standard for evaluating whether the subject community meets the intended standard in this regard, there is nothing in the standing test that would preclude consideration of similar factors.

#### *4.3.2. "Strong Association" between the Community and the gTLD String*

54. Both the standing test and the merits tests also require the Objector to demonstrate that there be a "strong association" between the subject community and the gTLD string. Specifically:

[15] Guidebook (Module 3), Section 3.2.2.4.

[16] Guidebook (Module 3), Section 3.5.4.

[17] Guidebook (Module 3), Section 3.5.4.

(1) Section 3.2.2.4 (setting out the standing requirements) states: "The community named by the objector must be **a community strongly associated with the applied-for gTLD string** in the application that is the subject of the objection"; and

(2) Test number three of the four mandatory tests in section 3.5.4 requires that there be "a **strong association between the community invoked and the applied-for gTLD string**."

55. The merits test suggests that the factors that could be balanced by a panel to determine this test include but are not limited to:

- *Statements contained in application;*
- *Other public statements by the applicant;*
- *Associations by the public.*

It also indicates that "if opposition by the relevant community is determined, but there is no 'strong association' [or targeting relationship] between the community and the applied-for gTLD string, the objection must be dismissed."

56. While the standing test does not elaborate what factors might be considered in the analysis, it does not preclude consideration of the above, or any other relevant factors.

57. In my reading of the language of the test, an Objector does not need to prove that the applied-for new gTLD string is exclusively or even primarily targeted at the relevant community. Rather, the words of the rule require a "strong association" between the new gTLD string and the relevant community. Reading the rule according to its plain language, I believe this to be the more reasonable interpretation.

## 5. ANALYSIS

### 5.1. Standing Analysis

#### *5.1.1. Established Institution*

58. The Objector must first demonstrate that it is "an established institution." The Objector asserts that it is, and I agree.

59. Section 3.2.2.4 indicates that a panel may consider the following non-mandatory and

non-exclusive factors as relevant to its determination on this issue:

(1) *Level of global recognition of the institution;*

(2) *Length of time the institution has been in existence; and*

(3) *Public historical evidence of its existence, such as the presence of a formal charter or national or international registration, or validation by a government, inter-governmental organization, or treaty. The institution must not have been established solely in conjunction with the gTLD application process.*

60. In arguing that it is an "established institution," Objector has asserted:

> *There is no question that CTIA is an "established institution" with an "ongoing relationship" with the clearly delineated Mobile Wireless Community. CTIA was founded in 1984, shortly after the first commercial cellular systems began operating, and has represented the interests of the mobile industry since that time. An international organization, with its primary regulatory focus in North America, it has nonetheless been globally recognized and active throughout its history.*
>
> *CTIA is a voluntary association composed of 256 companies, falling into three categories: Carrier members are those companies that hold a license or construction permit from the FCC or other North American regulatory body to offer commercial mobile services. Supplier members are those companies that provide services or equipment to the commercial mobile radio services or wireless Internet industries or engage in wireless Internet business activities. Associate members are those companies or organizations that provide mobile wireless service beyond North America or are consultants, resellers, academia, law firms, engineers, etc., working with the industry. Almost a quarter of all of CTIA's members have some foreign ownership and more than half operate globally, providing products and services to governments, companies, and individual users in more than 170 countries worldwide. A list of current CTIA members is attached. Attachment A.*
>
> *CTIA's Board of Directors draws upon the mobile network operators (aka "carriers") and suppliers who are members of CTIA. The list of CTIA's current Board is attached. A leadership team comprised of the President/CEO and eleven vice presidents head up the various CTIA departments and other operations, as discussed in more detail below. The CTIA Office of General Counsel provides legal counsel to all CTIA Departments and also manages outside counsel when necessary. A professional staff runs the Association and sees to the needs of its members.*[18]

[18] Objection, pp. 4-5.

61. Applicant has responded that Objector has failed to prove that it is an "established institution" as required by subsection 3.2.2.4 of the Guidebook.[19] In particular, Applicant points out:

> *With respect to the Guidebook's requirement that an objector be "an established institution," the Objector here has failed to provide any evidence for at least two of the three factors to consider in making this determination. Specifically:*
>
> *1. Guidebook Factor: "Level of global recognition of the institution." The Objection contains no evidence of global recognition of the Objector.*
>
> *2. Guidebook Factor: "Public historical evidence of its existence, such as the presence of a formal charter or national or international registration, or validation by a government, inter-governmental organization, or treaty." Other than an unsupported statement that it is "an international nonprofit membership organization," Objector has provided no historical evidence of its existence, that is, no formal charter or national or international registration and no validation by a government, inter-governmental organization, or treaty. Although Objector states that it has existed "since 1984" (Objection, p. 4), Objector provides no evidence of this or when its activities began in earnest.*[20]

62. However, I find that the evidence seems clear that Objector is an established, fully functioning, active and well-regarded entity with a robust and impressive membership and lineup of business activities. For instance, among other things:

(1) Objector appears to have been founded in 1984 and has developed a substantial membership roster and purview of activity.

(2) Objector has submitted into evidence a list of its 256 purported members as "Attachment A." Objector lists AT&T, Verizon Wireless, Sprint Nextel Corporation, T-Mobile USA among others as its "Carrier Members," and such names as Apple, Inc., LG Electronics, HTC America, Intuit, Nokia, Qualcomm, Research in Motion, and other household names among its "Supplier Members." The Applicant has not challenged the veracity of this member roster and I am not aware of any other challenges from any quarter despite the fact that this membership list is presented daily to the public on Objector's website as well as in connection with this new gTLD Program. Were it fraudulent in any material respect, one would expect that some interested party would have mentioned it.

[19] Response, p. 4.

[20] Response, p. 5.

Therefore, I take it to be accurate. The membership list alone is strongly supportive of the conclusion that Objector is an "established institution."

(3) Objector holds major trade shows annually with tens of thousands of attendees. Although Objector has not indicated "when its activities began in earnest", as Applicant would have it do, these trade shows are objectively verifiable events and, again, one does not build such well-attended trade shows overnight. Nor does one operate and maintain such major trade shows without an established organization and experienced staff. Again, this suggests that Objector is an "established institution."

63. I also find that Objector is globally recognized within its trade area. Its member roster contains numerous companies which are global brands, as mentioned above. Indeed, its Associate Members include "companies or organizations that provide mobile wireless service beyond North America." Such members include China Telecommunication Technology Labs , Hyper Taiwan Technology Inc., Lenovo Inc., TUV Rheinland Group and others, all of whom plainly have an international or global connection. Objector represents that these "Associate members include companies which provide, either directly or through their affiliates, mobile wireless service to more than 1 billion people in Asia, Africa, Europe, Central and South America" and that "almost a quarter of all of CTIA's members have some foreign ownership and more than half operate globally, providing products and services to governments, companies, and individual users in more than 170 countries worldwide."[21] While these statistics are not supported by specific evidence, there is sufficient evidence in the member list alone to make them at least plausible.

64. Objector also asserts that its most important activities are in policy-setting for the industry. It states that:

> *CTIA and its senior leadership meet regularly with key policymakers, government representatives, and trade representatives from the U.S. and around the world. In addition to regular contacts with the U.S. Administration, Congress, the Federal Communications Commission, and other federal agencies, members of CTIA's leadership team and senior staff have briefed representatives of the governments of the Federal Republic of Germany, Islamic Republic of Pakistan, Japan, People's Republic of China, Republic of Chile, Republic of Korea, the Russian Federation,*

[21] Objection, p. 5.

> *the Socialist Republic of Vietnam, State of Israel, and the United Kingdom, among others, on the mobile industry.*[22]

65. Overall, given that the bulk of the representations and evidence provided by Objector in support of its standing arguments consists of website content and other content generated by Objector, one might take a skeptical view of it, as the Applicant has. However, I have noted that Objector has also cited and attached a letter to the ICC International Centre for Expertise from Group Speciale Mobile Association ("***GSMA***"), dated 13 March 2013,[23] which indirectly serves to corroborate Objector's representations.

66. The GSMA is a premier global trade association that is widely known and well regarded in connection with mobile wireless technology and industry. The Director General of the GSMA writes to lend the GSMA's support to the Objection, stating:

> *On behalf of the GSMA, I write to affirm our opposition to the applications of Amazon EU S.a r.l. ("Amazon") and Dish DBS Corporation ("Dish") for the new gTLD string .MOBILE on the grounds that both Amazon and Dish have proposed to operate that TLD on a completely "closed" basis, making it unavailable to the vast majority of participants in the mobile services industry and members of the Mobile Wireless Community. As the major trade association for mobile operators around the globe, GSMA submits that granting exclusive rights in .MOBILE will harm competition in the mobile services marketplace and expose mobile subscribers to the likelihood of confusion and deception in their choice of mobile services and providers. As a result, consumers, our members, and other members of the Mobile Wireless Community will be harmed.*
>
> *The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities.*
>
> *We strongly agree with US Trade body CTIA - The Wireless Association® that the new gTLD will be closely identified with our Mobile Wireless Community and .MOBILE must not be reserved for the exclusive use of a single market participant. Accordingly, we fully support CTIA's objection to the Amazon and Dish Applications. [Emphasis added.]*

67. There is an implicit recognition in the GSMA's letter of the Objector's status in the

[22] Objection, p. 6.

[23] Objection, Attachment D.

trade. That the GSMA letter takes no pains to introduce the Objector except as "US trade body" would seem to suggests that no more introduction than this is required, thus giving credence to Objector's own representations about its status. GSMA agrees with the Objector that the .MOBILE string "will be closely identified with our Mobile Wireless Community." The reference to "our Mobile Wireless Community" lends further atmospheric support to this view. In short, the GSMA here has recognized the Objector as a U.S. trade body representing the so-called "Mobile Wireless Community" and lends its more explicitly global support.

68. In view of the above, along with other considerations reflected in the record, I find that Objector has shown that it is an "established institution" in satisfaction of the first standing requirement.

### *5.1.2. Ongoing Relationship with a Clearly Delineated Community*

69. The second prong of the standing test requires Objector to prove that it has an ongoing relationship with a clearly delineated community.[24] Objector contends that it has an ongoing relationship with what it calls the "Mobile Wireless Community," in satisfaction of the second required element for standing. I concur.

70. First, I consider the nature of the community (that is, whether the community is a clearly delineated one) and then the relationship of the Objector to that community (that is, whether it is an ongoing one).

#### 5.1.2.1. Clearly Delineated Community

71. I turn first to the community component of the test. "Community" is not defined in the Rules. It thus must be considered according to common usage and understanding of that term.

72. Although not raised by the parties, in my consideration of the issues, I have reviewed the comments of the Independent Objector ("***IO***"), whose role in the Program is to act "in the best interests of global Internet users" by "lodg[ing] objections in cases where no other objection has been filed."[25] The IO's comments are by no means binding or authoritative and I do not rely on them as such. But they are well-considered, widely

[24] Guidebook (Module 3), Section 3.2.2.4.

[25] See http://newgtlds.icann.org/en/program-status/odr/independent.

known, and publicly available for review by the parties. To the extent that the IO's comments reflect my own views concerning the concept of "community" in the context of the new gTLD Program dispute resolutions procedures, I comment on them here.

73. In commenting on Community Objections generally,[26] the IO has asserted that the "notion of 'community' is wide and broad" and may be generically described as "a group of individuals who have something in common," whether that be "common values, interests or goals (i.e. the health or legal community)." He further states: "[W]hat 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."

74. In the same comments, however, the IO also noted the difficulty of establishing a "clearly delineated community" that is associated with generic string terms. With regard to "generic terms" (such as the .MOBILE string), the IO takes the position that "it is unlikely that these applications will pass this community test" because "[b]y 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." Thus, the IO concludes, "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."

75. I share the view that a community may take a broad range of forms, and that an economic sector may be a form of community.[27] One may ask, though, what constitutes a "sector" of the economy that may be deemed a 'community'? To what extent must such an economic sector share common interests and activities? At what point is the linkage too tenuous to meet the "clearly delineated" threshold? And does the alleged "Mobile Wireless Community" as described by the Objector qualify?

[26] See http://www.independent-objector-newgtlds.org/home/the-issue-of-closed-generic-gtlds.

[27] I note that this same view was reflected in the ICANN Generic Names Supporting Organisation's Final Report on the Introduction of New Generic Top-Level Domains issued on 8 August 2007 (*"**ICANN Final Report**"*) which it indicates that the term 'community' "*should be interpreted broadly* and will include, for example, *an economic sector*, a cultural community, or a linguistic community. It may be a closely related community which believes it is impacted." (Emphases added.)

76. In this case, Objector has asserted that the "Mobile Wireless Community" is "a global community comprised of the carriers, network providers, and others involved in the delivery of mobile wireless and wireless-enabled services to governments, enterprises, and consumers worldwide." According to Objector, this community consists of Objector's members "and others like them." And what binds or links this community is a "common interest in the provision, enhancement and use of commercial mobile services, devices and applications."

77. I accept that there is a widely recognized sector of the global economy that is devoted to mobile wireless technologies. And, as I noted, an economic sector is a form of community. In this regard, Objector also declares that "[t]he community is well-defined and extensively studied as a critically important engine of the world economy." Had Objector included examples of the literature on this economic sector, it would make the task of evaluating the question of clear delineation simpler. But it has not, and so I undertake that analysis by other means.

78. Based on Objector's description of the "Mobile Wireless Community" and its other arguments, it considers the scope of the community to include parties as diverse as: wireless service providers such as AT&T, T-Mobile and Verizon, mobile device manufacturers and mobile app developers, among others. Objector states that "their common interest is the provision, enhancement and use of commercial mobile services, devices and applications."

79. It may be instructive to consider the diversity of Objector's membership, which is categorized as follows:

(1) "Carrier members are those companies that hold a license or construction permit from the FCC or other North American regulatory body to offer commercial mobile services."

(2) "Supplier members are those companies that provide services or equipment to the commercial mobile radio services or wireless Internet industries or engage in wireless Internet business activities."

(3) "Associate members are those companies or organizations that provide mobile wireless service beyond North America or are consultants, resellers, academia, law firms, engineers, etc., working with the industry."

80. Objector asserts that there is a common thread through all of its member groups, and that is that their activities are based in, or relate to, or depend on, the provision of wireless communications.

81. While a community will necessarily have some diversity—sometimes wide diversity—in its ranks, it may still be "clearly delineated." By being capable of circumscription, it is delineated. It should be possible in most cases to determine whether an entity is a carrier, network provider, or otherwise "involved in the delivery of mobile wireless and wireless-enabled services." This seems to me clearly delineated.

82. Indeed, it would appear that the GSMA has the same or similar conception of a "Mobile Wireless Community," since it makes a reference to "our Mobile Wireless Community" in its letter supporting the Objection.

83. However, it must be acknowledged that the mobile wireless industry is not as precisely circumscribed as certain other industries such as the insurance, banking or hotel industry, each of which is highly regulated and therefore very strictly delineated. While Objector's "Carrier Members," like a bank or insurance company, are easily identifiable because they must "hold a license or construction permit from the FCC or other North American regulatory body to offer commercial mobile services," the "Supplier Members" and "Associate Members" are more broadly inclusive. Applicant makes much of the wide breadth and diversity of the "Associate" category in particular as being "essentially unrestricted and open to anyone regardless of any affiliation with the wireless industry."

84. However, in my view it is not necessary that all of Objector's members must be considered as members of the Community in question. Under the Rules, it is sufficient that the objector be "associated with [a] clearly delineated"[28] community. The Rules do not suggest that such an association should be exclusive—i.e., that the objector may *only* be associated with members of the community at issue. It is therefore possible for an organization to be associated with a certain community even though certain members of the organization are not members of the community in question.

85. For instance, an academic interest alone does not make one a member of a

[28] Guidebook (Module 3), Section 3.2.2.4.

community; one can, for instance, study Judaism without being Jewish. But having said that, it is perfectly logical for a trade association representing an economic sector to invite and facilitate the involvement of academics and others who support and serve the community in various ways. Indeed, in my view it would not be fatal to the idea of a clearly delineated community if Objector did accept members who, as Applicant alleges, may have no "affiliation with the wireless industry" at all. (That said, as a practical matter it seems unlikely that anyone would make the investment to become a member of a trade association for an industry sector in which they have no interest.) Accordingly, I do not find the internal diversity of Objector's member categories to undermine the clarity of delineation of the community at issue. One can simply go back to the definition offered by the Objector: "carriers, network providers, and others involved in the delivery of mobile wireless and wireless-enabled services to governments, enterprises, and consumers worldwide." Does the entity or individual in question fall into that description or not?

86. One may say there is a bright line test: either one does provide mobile wireless services (or is involved in the provision of those services), or one does not. It is apparent to me that there is a community here that is substantially identifiable and, I think, recognizable to most, even though the exact boundaries may not be as precisely apparent as in certain highly regulated industries.

87. To further aid in my analysis of this issue, I evaluate each of the factors listed in section 3.5.4 relating to whether a community is "clearly delineated." Although section 3.5.4 sets out a set of factors to be considered for the merits test, for reasons asserted above, I find it appropriate to use them as a guide in the standing analysis on this point as well.

88. **First**, is there public recognition of the mobile wireless industry as a community at a local and/or global level? In my view, and based on the materials presented by the parties, there is unquestionably global recognition of the mobile or wireless economic sector generally.

89. **Second**, to what extent are there formal boundaries around the community, and what persons or entities are considered to form the community? Objector takes the position that its members "and others like them" form the community. In my view these "others" would include many of the members of the GSMA as well.

90. While the membership of the alleged "Mobile Wireless Community" would be wider than just the members of Objector and GSMA, the very process of joining and maintaining membership in trade associations or other groups certainly provides a formal process for those who choose it. Indeed, I consider the formality of organization of the community overall to be a relevant factor. In this case, the existence and scale of organizations such as Objector and the GSMA reflect a strong shared group interest in pursuing activities and policy goals that benefit the group as a whole. Such organizations only arise where there is a common interest in a community, and active participation.

91. Thus, while membership in the alleged "Mobile Wireless Community" does not *require* membership in Objector or any other organization, such organizational bodies do exist and, as noted above, the fee requirement and self-selection of the membership results in a natural exclusionary function such that the membership of such organizations will inevitably be substantially composed of community members.

92. **Third**, how long has the community been in existence? The "Mobile Wireless Community," as described by Objector, has been in existence for several decades, since mobile or wireless communications services and devices were made commercially available. According to Objector, this was in 1984. I accept this.

93. **Fourth**, what is the global distribution of the community (this may not apply if the community is territorial)? Objector has defined the community at issue as "global" and noted that it consists of its own members "and others like them." It further states:

> *CTIA's carrier members (mobile network operators and mobile virtual network operators) alone serve more than 304 million mobile wireless subscribers in the U.S., including customers using more than 300 million data-capable and more than 243 million web-capable devices. ... CTIA's non-carrier members provide mobile-related products and services worldwide, including mobile network infrastructure, mobile devices (handsets, tablets, mobile data modems), chipsets, software and content, and a wide variety of accessories and enabling technologies and components. In addition, CTIA's Associate members include companies which provide, either directly or through their affiliates, mobile wireless service to more than 1 billion people in Asia, Africa, Europe, Central and South America. In combination with CTIA's General members, CTIA's members provide mobile wireless service to more than 1.3 billion people worldwide.*[29]

[29] Objection, p. 5.

94. In addition, Objector has acknowledged that the alleged global "Mobile Wireless Community" consists of its members "and others like them," which would clearly also include the members of GSMA, which has also lent its support to the Objection. Therefore, I find that the invoked community is both substantial and globally distributed.

95. **Fifth**, what number of people or entities makes up the community? It is sufficient to say that, plainly, the number of people or entities that make up the community is large and is substantially reflected in the membership of the Objector and the GSMA.

96. For all these reasons, I find that there is a clearly delineated community, which is the "Mobile Wireless Community" as described by the Objector, consisting of "carriers, network providers, and others involved in the delivery of mobile wireless and wireless-enabled services to governments, enterprises, and consumers worldwide."

#### 5.1.2.2. Ongoing relationship

97. Having concluded there is a clearly delineated community, I next turn to the question of whether Objector has shown that it has an ongoing relationship with that community. I find that it has. Although it may not serve the entire community, it is the trade association for a very significant component of the community (i.e., the US/North American sub-community), as reflected in its extensive membership list and the many important companies that populate them.

98. Objector describes its major activities on behalf of the Mobile Wireless Community:

> *CTIA's activities since 1984 have included internationally-attended major trade shows and conferences. The most recent MobileCON™ and CTIA WIRELESS® shows (held in 2012) attracted more than 30,000 attendees including 4,170 foreign/international attendees.*
>
> *In addition to the two annual CTIA conferences, CTIA's departments and operations include:*
>
> *—The External and State Affairs Department is CTIA's liaison with state legislatures, regulatory entities and advocacy organizations on wireless communications issues.*
>
> *—The CTIA Government Affairs Department is the voice of the wireless industry on Capitol Hill and at various Executive branch departments and agencies.*
>
> *—The CTIA Operations Department consists of the CTIA Membership division, CTIA Technology Programs, and the CTIA Certification Program. In addition it produces the CTIA MobileCON™ and WIRELESS® conventions.*

> *—The CTIA Public Affairs Department serves as the voice of the wireless industry as the primary contact for members of the media, and functions as a communications resource to member companies, analysts, and national, local, and trade media.*
>
> *—The Regulatory Affairs Department is the chief representative of the wireless industry before the Federal Communications Commission and other federal government organizations that seek to regulate the wireless industry.*
>
> *—The Wireless Internet Development Department focuses on accelerating the growth of the wireless data segment of the industry, in large part by supporting the Wireless Internet Caucus (WIC).*
>
> *See http://www.ctia.org/aboutCTIA/structure/.*[30]

99. Objector further refers to its alleged development of international "certification programs" and "voluntary guidelines to protect mobile users".[31]

100. Finally, Objector describes its lobbying activities on behalf of the Mobile Wireless Community as follows:

> *Perhaps most importantly, representatives of CTIA and its senior leadership meet regularly with key policymakers, government representatives, and trade representatives from the U.S. and around the world. In addition to regular contacts with the U.S. Administration, Congress, the Federal Communications Commission, and other federal agencies, members of CTIA's leadership team and senior staff have briefed representatives of the governments of the Federal Republic of Germany, Islamic Republic of Pakistan, Japan, People's Republic of China, Republic of Chile, Republic of Korea, the Russian Federation, the Socialist Republic of Vietnam, State of Israel, and the United Kingdom, among others, on the mobile industry.*[32]

101. I note here, too, the contents of the GSMA letter dated 13 March 2013, quoted above, which lends support to the Objection.[33]

102. Applicant counters by arguing that Objector has failed to prove that it has an "ongoing relationship with a clearly delineated community" as required by subsection 3.2.2.4 of the Guidebook.[34] In particular, Applicant points out that Objector has "failed to provide evidence for at least three of the four factors to consider in making this

[30] *Id.* at 5-6.

[31] *Id.* at 6.

[32] *Id.*

[33] See Objection, Attachment D, third paragraph.

[34] Response, p. 4.

determination," and states:

> *Guidebook Factor: "The presence of mechanisms for participation in activities, membership, and leadership."* *Objector claims that it "is a voluntary association composed of 256 companies." (Objection, p. 5.) However, the Objection contains no information as to how (or even whether) any of these companies participate in activities, membership and leadership of the Objector, or what criteria exist for a company to become a member. Indeed, according to Objector's own website, membership is open to a tremendously broad range of individuals and companies, as diverse as "consultants, resellers, academia, law firms, engineers, etc." that are merely "working with the wireless industry" – and the "CTIA Associate Membership Application" does not even require that a member show how (or whether) it satisfies this broad criteria. Accordingly, it appears that membership in Objector's association is essentially unrestricted and open to anyone regardless of any affiliation with the wireless industry.*
>
> *Guidebook Factor: "Institutional purpose related to the benefit of the associated community."* *The Objection contains no information about the institutional purpose of the Objector or its alleged community, other than the fact that Objector "represent*[s]*" the wireless communications industry (Objection, p. 4) and the fact that its representatives "meet regularly with key policymakers, government representatives, and trade representatives from the U.S. and around the world." (Objection, p. 6.) These vague, broad and unsupported statements offer no information about the institutional purpose of the Objector or how it benefits any community.*
>
> *Guidebook Factor: "The level of formal boundaries around the community."* *Although the Objection refers to "the Mobile Wireless Community" (Objection, p. 4), the Objector fails to define this community. Further, as shown above and as set forth in the "CTIA Associate Membership Application," there are no formal boundaries around the community given that any person or company can become a member of Objector's association. The only eligibility criteria appear to be an ability pay Objector's annual dues of $6,000.*
>
> *In addition, as ICANN's Independent Objector has made clear, it is unlikely that a "clearly delineated" community exists around any generic term (such as "mobile") because "[b]y 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."*[35]

103. Applicant concludes: "In light of the above, it is apparent that Objector is ineligible to file the Objection in this proceeding and, for that reason alone, the Panel should deny

[35] Response, pp. 5-6.

the Objection."[36]

104. However, I am not persuaded by these arguments. I have directly addressed the objection in the first and third "Guidebook factors" above already. As to the second, while I agree that it would have served Objector's goals better for it to provide for extensive and concrete evidence of its activities and purposes, the simple fact of its robust membership lists is indicative of the fact that it is serving its role as trade association in the US successfully. Furthermore, that it is a "US Trade body" for the Mobile Wireless Community, as independently asserted by the GSMA, and is supported in its objection by the GSMA is sufficiently demonstrative of its role on behalf of the Mobile Wireless Community. The function of a trade association is generally understood,[37] though its specific activities may be diverse and varied. And the prominence and importance of the US in wireless and mobile communications worldwide is beyond dispute. From this, it can be inferred that it does serve an institutional purpose relevant to the designated community, and that for purposes of its Objection, it represents that community.

105. For all the reasons above, I find that Objector has demonstrated an ongoing relationship with the Mobile Wireless Community by virtue of its prominent role as the US trade association of that community, as also reflected in the support lent to its Objection by the GSMA.

### *5.1.1. Strong Association*

106. The third element required for standing is the existence of "a community strongly associated with the applied-for gTLD string" objected to. As noted above, the merits tests likewise include a component requiring a "strong association" between the specified community and the gTLD string at issue.

107. I would add one note of clarification regarding this requirement, and that is that the threshold is a relatively high one—"strong" association—but it by no means requires that the gTLD string must be an identifier that is unique to the community at issue.

108. The word "mobile" of course has various meanings. Applicant has cited Merriam-

[36] *Id.*, at 6.

[37] See, e.g., http://www.wisegeek.com/what-is-a-trade-association.htm.

Webster's online dictionary in which the first six adjectival definitions of "mobile" and the single noun definition make no reference to wireless communications or devices. But these kinds of results can be cherry-picked. By contrast, Objector has noted that the first search result in Google is T-Mobile. Different sources produce different results. The Wikipedia entry for "mobile," for instance, begins as follows:

> **Mobile** often refers to:
>
> - Mobile phone, a portable communications device
> - Mobile, Alabama, a U.S. port city
> - Mobile (sculpture), a hanging artwork (or toy)
> - Mobility, the ability to move or be moved
> - Mobility of single cell animals (motility)
> - Mobile forces, especially Motorized infantry or Mounted infantry
>
> **Mobile** may also refer to:
>
> **Technology**
>
> - Mobile computing, a generic term describing one's ability to use technology in mobile environments
> - Mobile device, a computer designed for mobile computing
> - Mobile game, a video game played on a mobile phone, smartphone, PDA or handheld computer
> - Mobile Magazine, a publication on portable electronics
> - Mobile network operator, a company which provides mobile phone network access and services
> - Mobile radio, wireless communications systems and devices which are based on radio frequencies
> - Mobile rig
> - Mobile station, user equipment and software needed for communication with a wireless telephone network
> - Mobile Web, the World Wide Web as accessed from mobile devices using Mobile Web Browser
> - Mobile TV, TV services viewed via a mobile device.[38]

109. Indeed, in the internet world within which the new gTLDs will operate, the association of the term "mobile" with wireless technologies may predominate over more traditional or historical meanings of the word. It is not uncommon for people in

[38] Following the above are additional usage categories "places" and "entertainment." See http://en.wikipedia.org/wiki/Mobile.

countries where such technologies are common to use the word “mobile” as a synonym for a cellular phone on business cards or in conversation, and “mobile device” is commonly used to capture the category of technological devices which operate via wireless communications signals, such as cellular phones, smart phones, tablets, and the like. Such contemporary usage is heavily reflected in the Wikipedia page excerpt above.

110. In this regard, Objector has asserted:

> *There is a "strong association" between the Mobile Wireless Community and the .MOBILE gTLD string because the term "MOBILE" is plainly descriptive of the key defining characteristic of the products and services which the Community provides. CTIA's member companies, both carrier and non-carrier, are significantly engaged in the mobile industry in the United States and globally. This engagement involves the provision of mobile offerings to end users in the form of mobile services, mobile equipment, and other mobile-enabled and mobile-related products (i.e., mobile commerce).*
>
> *These products include the production and sale of mobile applications to end-users and, as previously noted, more than one billion mobile devices including mobile handsets, mobile data modems, and other mobile devices used worldwide. MobileCON™, as discussed above, is a key CTIA conference. Further, the number one Google search result for "mobile" is the homepage of T-Mobile, which profiles its mobile devices and services. Attachment E.*
>
> *Additional, CTIA's Mobile Application Rating System, is "a rating system specifically designed for mobile applications." See http://www.growingwireless.com/learn-engage/ctia-mobileapplication-rating-system-with-esrb. CTIA also has endorsed the U.S. Federal Trade Commission's 'Marketing Your Mobile App' Guidelines (Sept. 2012) at http:www.ctia.org/media/press/body.cfm/prid/2206.*
>
> *Indeed, despite the fact that there are "fixed" wireless services as well, "mobile" and "wireless" are often used interchangeably both within the industry and by the public at large. For example, Bing searches for "mobile" produce numerous ads for cellular telephone services. Thus, it is fair to say that telecommunications mobility represents the common interest and link among all of the members of the Community. The GSMA "strongly agree[s] with US Trade body CTIA-The Wireless Association® that the new gTLD will be closely identified with our Mobile Wireless Community and .MOBILE must not be reserved for the exclusive use of a single market participant." Attachment D.*[39]

111. Respondent has denied that Objector has shown a strong association between the string and the targeted community, stating:

[39] Objection, p. 8.

> *Objector has failed to prove "a strong association between the applied-for gTLD string and the community represented by the objector," as required by the Guidebook, subsection 3.5.4.*
>
> *Objector indicates that it "represent[s] the wireless communications industry" (Objection, p. 4) and that its "carrier and non-carrier" members "are significantly engaged in the mobile industry" (Objection, p. 8); however, the Objector does not provide any evidence that the .mobile gTLD is strongly associated with this community. Indeed, although the Guidebook provides three factors to consider when evaluating such targeting, the Objector has not provided any information relevant to any of these three factors – because all three factors weigh against the Objector. Specifically:*
>
> *1. <u>Guidebook Factor: "Statements contained in the application."</u> The Application states that the mission of the .MOBILE registry is as follows:*
>
> *To provide a unique and dedicated platform for Amazon while simultaneously protecting the integrity of its brand and reputation.*
>
> *A .MOBILE registry will:*
>
> *●Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.*
>
> *●Provide Amazon a further platform for innovation.*
>
> *●Enable Amazon to protect its intellectual property rights.*
>
> *Application, para. 18(a).*
>
> *Nowhere in the Application does the Applicant make reference to the words or phrases "wireless," "carrier," "communications industry" or "mobile industry."*
>
> *Accordingly, there are no statements in the Application indicating an association (let alone a "strong association") between the applied-for gTLD and the community represented by the Objector.*
>
> *2. <u>Guidebook Factor: "Other public statements by the applicant."</u> The Objection does not refer to any public statements made by the Applicant regarding the Application, because Applicant has made no such public statements.*
>
> *3. <u>Guidebook Factor: "Associations by the public."</u> The Objection does not contain evidence of any associations by the public that the applied-for gTLD targets the community represented by the Objector. In any event, the word "mobile" has many definitions that do not bear any association with the wireless communications industry, as shown in the printout attached hereto as Annex 8, from the website of the Merriam-Webster dictionary. Indeed, the first six definitions of "mobile" as an adjective are unrelated to the wireless communications industry, as is the only definition of "mobile" as a noun*[.][40]

112. I am not aware of any statements by Applicant in its Application or otherwise linking the Application with the Mobile Wireless Community. Rather, the Application

[40] Response, pp. 8-9.

specifically indicates that it is not a "community-based" application. Therefore, there is no need to even consider the first two objections raised by Applicant above. As to the associations of the public, for reasons I have asserted above and with the arguments of Objector also in mind, I find that there is a strong association in the public mind between the word "mobile" and the Mobile Wireless Community as defined by Objector.

113. In conclusion, I find that the word "mobile" is strongly associated with the Mobile Wireless Community as it has been defined by Objector, thus satisfying this test.

### *5.1.2. Sub-conclusion*

114. In conclusion, Objector has satisfied all three criteria to have standing to submit its Community Objection.

## 5.2. Merits Analysis

### *5.2.1. Clearly Delineated Community*

115. As noted above, this requirement is present both in the standing and merits tests. I have already conducted the necessary analysis for standing, which is sufficient for merits purposes as well. Therefore, I shall not repeat it here, but simply restate that Objector has demonstrated satisfactorily that the Mobile Wireless Community is a clearly delineated community as required by the Rules.

### *5.2.2. Substantial Opposition by the Community*

116. Objector asserts that there is substantial opposition from the target community, in satisfaction of this test—the second of four mandatory tests. I agree.

117. Under this test, the Objector "must prove substantial opposition within the community it has identified itself as representing."[41] The expert may balance a number of factors to determine whether there is substantial opposition, including but not limited to:

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

[41] Guidebook (Module 3), Section 3.5.4.

- *The representative nature of entities expressing opposition;*
- *Level of recognized stature or weight among sources of opposition;*
- *Distribution or diversity among sources of expressions of opposition, including:*
    - *Regional*
    - *Subsectors of community*
    - *Leadership of community*
    - *Membership of community*
    - *Historical defense of the community in other contexts; and*
- *Costs incurred by objector in expressing opposition, including other channels the objector may have used to convey opposition.*[42]

118. If some opposition within the community is determined, but it does not meet the standard of substantial opposition, the objection will fail.[43]

119. In support of its assertion that there is substantial opposition in the Mobile Wireless Community, Objector asserts:

> *CTIA's opposition alone constitutes substantial opposition to the Amazon application from the Mobile Wireless Community because of the breadth of its membership and its leading stature in that Community. CTIA's opposition is entitled to substantial weight as the Association represents companies across the mobile ecosystem, including mobile network operators and mobile virtual network operators serving more than 304 million subscribers in the United States and its territories, and suppliers of mobile network infrastructure and devices responsible for the production of more than 1.1 billion mobile devices that were sold to end users worldwide in 2012. See Gartner Press Release,* Gartner Says Worldwide Mobile Phone Sales Declined 1.7 Percent in 2012, *Feb. 13, 2013. Attachment C. Including members' owners and affiliates, CTIA-related providers serve more than 1.3 billion subscribers worldwide. Together with the GSMA, there are more than 3.2 billion mobile wireless users worldwide. See http://gsmamobileeconomy.com/.*
>
> *CTIA's members also include non-traditional platform providers who offer more than 1.5 million mobile applications to end users worldwide, and suppliers of chipsets, software and other content, and a wide variety of accessories and enabling technologies and components essential to the provision to and enjoyment of mobile service by users worldwide. Accordingly, in no way can the opposition of these significant global industry elements/community members to the Amazon application for a "closed" .MOBILE gTLD be deemed insubstantial.*

[42] *Id.*

[43] *Id.*

> *Notably, the world's largest mobile services trade association fully supports CTIA's objection and opposes Amazon's application. The Groupe Speciale Mobile Association ("GSMA") "represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities." The GSMA affirms its "opposition to the Application[] of Amazon EU S.a r.l. ... for the New gTLD string .MOBILE on the grounds that ... Amazon ...* [has] *proposed to operate that TLD on a completely 'closed' basis, making it unavailable to the vast majority of participants in the mobile services industry and members of the Mobile Wireless Community. As the major trade association for mobile services operators around the globe, GSMA submits that granting exclusive rights in .MOBILE will harm competition in the mobile services marketplace and expose mobile subscribers to the likelihood of confusion and deception in their choice of mobile services and providers. As a result, consumers, our members, and other members of the Mobile Wireless Community will be harmed." Attachment D.*[44]

120. Applicant disagrees, asserting:

> *Objector has failed to prove that there is "substantial opposition within the community it has identified itself as representing," as required by the Guidebook, subsection 3.5.4. Specifically, Objector has failed to prove or even provide adequate evidence of any of the six factors to determine whether there is substantial opposition, namely:*
>
> *1. <u>Guidebook Factor: "Number of expressions of opposition relative to the composition of the community."</u> Other than a single letter from a European-based trade association, Objector has provided **<u>no evidence of any expressions of opposition from the community</u>**. Furthermore, it cannot be assumed that all of Objector's members support the Objection. For example, while Objector's online membership list identifies "Google Inc" as a member, Google has been conspicuously omitted from the list of members included by the Objector as <u>Attachment A</u> to the Objection, raising the question as to whether Google and/or other members specifically oppose the Objection.*
>
> *2. <u>Guidebook Factor: "The representative nature of entities expressing opposition."</u> Because, as stated above, Objector has failed to identify any entities other than a European-based trade association that supports its Objection, it is impossible to evaluate the "representative nature" of any such entities. Further, as also stated above, the worldwide base of mobile phone subscribers is about six billion, so it is far from likely that the Objector adequately represents the interests of such a diverse group.*
>
> *3. <u>Guidebook Factor: "Level of recognized stature or weight among sources of opposition."</u> Objector has not provided any information as to this factor.*

[44] Objection, p. 8.

> *4. <u>Guidebook Factor: "Historical defense of the community in other contexts."</u> The Objection contains no information whatsoever as to how or even whether it has defended the wireless community in any context. Indeed, the activities described by the Objector – conferences, lobbying and public relations (Objection, p. 5-6) – are general and proactive in nature and not in any way defensive.*
>
> *5. <u>Guidebook Factor: "Costs incurred by objector in expressing opposition, including other channels the objector may have used to convey opposition."</u> Not only has Objector failed to include any information about costs it may have incurred in expressing opposition to Applicant's Application for the .mobile gTLD, but the Objection contains no references to any other channels that Objector has used to convey opposition. Indeed, despite a three-month window during which the public was invited to submit comments on all of the gTLD applications (a process that resulted in 12,160 comments), Objector did not submit any comments on the Applicant's .mobile Application.*[45]

121. I find that this test is satisfied in the overall circumstances. In particular, as I have discussed above, it is apparent to me that Objector serves an important representative function in the Mobile Wireless Community as a US trade association that acts as the policy-guiding and lobbying arm of the industry, the central organizer of two of the largest trade shows in the industry in North America, and in certain other capacities. Accordingly, the opposition of Objector alone may be sufficient to meet the "substantial opposition" test.

122. Moreover, in addition to the Objector, the GSMA (the largest, global trade association in the Mobile Wireless Community) and others have expressed objections to the Application for the .MOBILE gTLD on the grounds that it should not be operated as a so-called "closed generic gTLD." Between the Objector and the GSMA, there is plainly "substantial opposition" to the Application for the .MOBILE gTLD.

### *5.2.3. Strong Association ("Targeting")*

123. This test requires the Objector to "prove a strong association between the applied-for gTLD string and the community represented by the objector."[46] As I explained above, the tests for standing and merits both contain almost identical phraseology and I find that the same analysis can be applied to both with the same result. Rather than repeat the analysis here, I refer to my analysis on this requirement in the standing section above, and confirm that I find that Objector has proven a "strong association between

[45] Response, pp. 7-8.

[46] Guidebook (Module 3), Section 3.5.4.

the applied-for gTLD string and the community represented by the objector" in satisfaction of this test on the merits.

### *5.2.4. Likelihood of Material Detriment*

124. To satisfy this test, the Objector must "prove 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."[47] It is further clarified that "[a]n allegation of detriment that consists only of the applicant being delegated the string instead of the objector will not be sufficient for a finding of material detriment."

125. Factors that could be used by a panel in making this determination include but are not limited to:

> •*Nature 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;*
>
> •*Evidence that the applicant is not acting or does not intend to act in accordance with the interests of the community or of users more widely, including evidence that the applicant has not proposed or does not intend to institute effective security protection for user interests;*
>
> •*Interference with the core activities of the community that would result from the applicant's operation of the applied-for gTLD string;*
>
> •*Dependence of the community represented by the objector on the DNS for its core activities;*
>
> •*Nature and extent of concrete or economic damage to the community represented by the objector that would result from the applicant's operation of the applied-for gTLD string; and*
>
> •*Level of certainty that alleged detrimental outcomes would occur.*[48]

126. The list of factors above is, again, non-mandatory and non-exclusionary. It includes actual economic harm, reputational harm, the potential for Applicant to act inconsistently with the community's interests "or of users more widely", actual interference with the community's activities, a forced dependency relationship, etc.

127. In support of its argument that the Mobile Wireless Community will likely suffer

[47] Guidebook (Module 3), Section 3.5.4.

[48] Guidebook (Module 3), Section 3.5.4.

material detriment, Objector asserts that "exclusive access of one company to all domain names within the .MOBILE TLD will have a substantial impact in the marketplace and lead to real and significant harm and material detriment for the Mobile Wireless Community." Objector presents its arguments in support of this contention in several sub-sections, as follows. Rather than recite Objector's extensive arguments in each case, I insert my views and findings under each heading, reflecting my pertinent views and findings in response to Applicant's arguments as well. While I do not address each and every argument asserted, I have reviewed and considered them all in reaching my conclusions.

#### 5.2.4.1. Amazon Has Expressly Acknowledged That It Has No Intention of Operating The .MOBILE gTLD In Accordance With The Interests Of The Mobile Wireless Community.

128. It is not disputed that under the Application, Applicant has declared an intention to operate the registry on a closed basis for its own use. As noted above, there is some indication that Applicant will not—or will be precluded from—doing this. But the actual outcome is far from clear and, in any event, is beyond the purview of my mandate as Expert. Therefore, I find that the evidence suggests that Applicant will not act in accordance with the interests of the Mobile Wireless Community to the extent that the community has an interest in exploiting .MOBILE domain names.

129. Given the fact that, as discussed above, there is a "strong association" between the string and the Mobile Wireless Community, this would inherently have some effect on the community. Among other things, it would be indefinitely precluded from making use of the very gTLD that is strongly associated—perhaps most strongly associated—with it.

130. While it is at present easy to argue that the Mobile Wireless Community would not be harmed because they can simply conduct their business under .COM or other gTLDs as they do now, that argument is circular. .MOBILE domain names have no present quantifiable value because they do not yet exist. The same could be said universally of any market entrant today, which could simply select a domain name using presently available gTLDs. However, the very fact that market forces have pressed for additional gTLDs strongly suggests that new gTLDs are wanted and, by virtue of being wanted, will have market value. In light of the present Program, it is not difficult to reach the conclusion that once the geography of the domain name landscape changes with the

addition of new gTLDs through the current program (of which this is only the first round), industries and market participants will begin to use these as identifiers rather than sticking with the one-size-fits-all .COM or equivalents. In the expanded-gTLD internet world, in light of the Mobile Wireless Community's strong association with the term "mobile," it is very likely to want access to the .MOBILE gTLD. This is indicated, among other reasons, by the fact that the community's advocates say so now, and object to the Applicant having exclusive access to it. In my view, if Applicant is permitted to lay exclusive claim to all .MOBILE domain names it would constitutes a likely material detriment to the Mobile Wireless Community.

#### 5.2.4.2. Access to the .MOBILE Domain Names, in the Highly Competitive Mobile Marketplace Is Critical to the Core Activities of the Mobile Wireless Community – a Community Heavily Vested in and Dependent on the DNS

131. I am not certain that having access to the .MOBILE gTLD is "critical to the core activities of the Mobile Wireless Community"—at least at this point in time. If it was, one would expect that community to swiftly move to submit its own application to act as the register itself. However, as the domain name landscape adjusts to the expanded gTLD options, this may well become the case. In any case, as explained above, in my view it is likely to have value to the Mobile Wireless Community. The gTLD .MOBILE is not a generic descriptor like ".com" (short for "company"), but an identifying descriptor that is a widely used to refer to the community. (Indeed, while not determinative in any way, it is noteworthy that the .MOBILE string has a far weaker association with Amazon than it does with the Mobile Wireless Community.) Within the bounds of the Mobile Wireless Community, .MOBILE could easily function in a manner similar to the way .COM functions in the broader internet economy.

132. Top-level domain names are not co-equal with the second-level name market. There, excepting certain limitations and preclusions, one need only find a unique name and pay to register it. However, a TLD is something else entirely. A market participant cannot simply "register" a TLD like .MOBILE or .WIRELESS or .APP, as it can register a second-level domain name like "app.com." Rather, one must become the registrant, which is an expensive, time-consuming, complex process. And after a registrant is selected, it cannot simply sell its rights as a registrant to another market participant. It is a highly regulated position, subject to the oversight of ICANN and to numerous regulations.

133. Hence, it is incorrect to say that Amazon's securing the .MOBILE gTLD is no different than the AT&T's registering the MOBILE.COM domain name. It is for this reason, it seems to me that ICANN has provided affected communities the opportunity to object where the community fulfills the requirements contained in the Guidebook.

134. As stated in the list of factors above, material detriment may be shown, among other things, where there is "[e]vidence that the applicant is not acting or does not intend to act in accordance with the interests of the community or of users more widely, including evidence that the applicant has not proposed or does not intend to institute effective security protection for user interests." In this case, Applicant has proposed no effective security protections for the simple reason that its Application proposes not to allow the Mobile Wireless Community—or other users—access to the .MOBILE gTLD at all.

135. The establishment of unrestricted, exclusive rights to a gTLD that is strongly associated with a certain community or communities, particularly where those communities are, or are likely to be, active in the internet sphere, seems to me inherently detrimental to those communities' interests. And it is unquestionably the case that the Mobile Wireless Community is a community for which domain name "real estate" is of high value.

#### 5.2.4.3. The Mobile Wireless Community Will Suffer Significant and Extensive Economic Harm Should .MOBILE Be Delegated to Amazon Under the Terms Set Out in the New gTLD Application

136. While I do not necessarily agree with all of the potential harms foreseen by Objector, I am persuaded that .MOBILE is a highly descriptive term which, if Applicant alone has access, it will have the power to exploit to its advantage while denying the opportunity to the Mobile Wireless Community which has a strong interest in it.

137. In this regard, I feel compelled to clarify that I am not taking the position that there should or can be no closed registry of generic terms at all. That is a policy question for others to determine. I only take the view that in a case such as this where a party has shown that it is a community strongly associated with a particular gTLD and there is substantial opposition in that community to a particular party having a closed registry on that gTLD, there is a strong likelihood that there is a material detriment.

#### 5.2.4.4. The Level of Certainty That the Alleged Harms Will Occur Is Very High

138. Based on the Application and Response of Applicant, it is clear that Applicant will, if granted the .MOBILE registry, operate it for its own exclusive benefit, and the Mobile Wireless Community will be precluded indefinitely from using this gTLD. In my view, given the strong association between .MOBILE and the Mobile Wireless Community in the mind of the internet public, there is a high likelihood that this will result in the detriment discussed above.

### *5.2.5. Sub-conclusion*

139. In conclusion, I find that Objector has satisfied each of the four tests on the merits of the Objection. Accordingly, its Objection is successful.

## 6. EXPERT DETERMINATION

140. Based on the foregoing, I decide that the Objector has standing and has satisfied the four tests required for a successful Community Objection.

141. Therefore, Objector has prevailed and the Objection is upheld. As the Objector is the prevailing party, the Centre shall refund the Objector's advance payment of costs to the Objector in accordance with Article 14(e) of the Procedure.

Date of Signature: 10 April 2014

Kap-You (Kevin) Kim
Expert

# Appendix B

.MUSIC (DotMusic Limited) Reconsideration Request Against Community Objection Decisions Relating to Amazon's Music-Themed Exclusive Access Applications

# Reconsideration Request Form

## 1. Requester Information

**Name: Constantinos Roussos**

**Address:** Contact Information Redacted

**Email:** Contact nformation Redacted **with a copy to counsel,** Contact Information Redacted

## 2. Request for Reconciliation of:

__X__ **Staff action/inaction**

## 3. Description of specific action you are seeking to have reconsidered.

DotMusic is challenging ICANN's inaction on 3 issues:

1) In not properly supervising and ensuring that appropriately qualified Expert candidates of the International Chamber of Commerce ("ICC") were a) selected; and b) adequately, trained to address the unique issues presented by Community Objections and the gTLD Program. The community expected that the ICC would be required to appoint and advise an appropriately qualified "expert," (not just an arbitrator) familiar with the unique needs and requirements presented in the gTLD Program, intellectual property and anti-competitive issues, and the needs and composition of the relevant community (e.g. a music or intellectual property expert for music-themed Objections)(Point 1);

2) In not recognizing the relevance and impact of the exceptional GAC Advice on the Community Objection process and Community Applicants, and in not advising the ICC and Community Objection Panelists on the GAC Beijing Communique of April 11, 2013 and subsequent GAC related issues: Responses to GAC Advice, Board Resolutions, Material Changes in Applicant positions through their GAC Advice Category 2 Exclusive Access Responses, and revisions to the new gTLD Registry Agreement[1] that addressed GAC

[1] 3(c) and 3(d) of Specification 11 provided that: (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

Concerns pertaining to exclusive access which were directly related to the anti-competitive issues raised in Community Objections. (Point 2); and

3) In not creating an appropriate appeal process for Community Objections and denying parties procedures to protect their fundamental rights and legitimate interests (Point 3).

**4. Date of action/inaction:**

The relevant Expert Determinations EXP_461_ICANN_78 (c EXP_479_ICANN_96 EXP_480_ICANN_97) were published on December 9, 2013 (See Annex 1).

**5. On what date did you became aware of the action or that action would not be taken?**

The Decisions were presented to Objector and made public on December 9, 2013.

**6. Describe how you believe you are materially affected by the action or inaction:**

DotMusic Limited is a privately-held Cyprus limited liability company representing Community Objectors and Related-Objector Entities in Community Objections. Objector and/or Related-Objector Entities constitute a significant portion of the music community.[2]

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" [. . .]. "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 others" (New gTLD Registry Agreement, July 2nd, 2013, https://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm#1.d).

[2] Objector Associate members include Pandora (http://a2im.org/groups/pandora), the world's largest streaming music radio with over 72 million active members (http://investor.pandora.com/phoenix.zhtml?c=227956&p=irol-newsArticle&id=1860864) and Apple iTunes (http://a2im.org/groups/itunes). iTunes accounts for 63% of global digital music market (http://appleinsider.com/articles/13/04/16/apples-itunes-rules-digital-music-market-with-63-share) – a majority - with 575 million active global members (http://appleinsider.com/articles/13/06/14/apple-now-adding-500000-new-itunes-accounts-per-day) abiding to strict terms of service and boundaries (http://www.apple.com/legal/internet-services/itunes/ww/index.html) have downloaded 25 billion songs from iTunes catalog of over 26 million songs, available in 119 countries, regardless whether artist is independent or in a major label (http://www.apple.com/pr/library/2013/02/06iTunes-Store-Sets-New-Record-with-25-Billion-Songs-Sold.html). Related Objector Entities include: an international federation of nearly 70 government ministries of culture and arts councils, music distributors that distribute over 70% of global music on retailers such as iTunes and Amazon (e.g. Tune core, with over 500,000,000 sales, distributes more music in one month than all major labels have combined in 100 years, http://blog.tunecore.com/2012/02/what-the-riaa-wont-tell-you-tunecores-response-to-the-ny-times-op-ed-by-the-riaa-ceo-cary-h-sherman.html), an international association of music information offices from over 30 countries, music coalitions from leading music territories such as Canada, Brazil, France and others, music communities representing over 3 million musicians, industry professionals and organizations, the national association of recording industry professionals and others (http://music.us/supporters.htm).

The American Association of Independent Music is a non-for profit company representing its Members (both Labels and Associates), the U.S. Independent label music community, the World Independent Network, the Association of Independent Music, the Independent Music Companies Association (IMPALA) and the Merlin Network who collectively constitute a majority of the music community (emphasis added) to which the string is explicitly or implicitly targeted. (the "Affected Parties").

On the 13th of March, 2013 Objections (cases EXP_461_ICANN_78 (c EXP_479_ICANN_96 EXP_480_ICANN_97) were filed against Amazon EU S.A.R.L in connection with music-themed Applications to run an exclusive access registry for .music, .song and .tunes (the "Objections"). The Objections raised concerns, among other things, about Applicant's Applications to run exclusive-access registries thereby controlling the most semantically significant music-themed-strings and an entire scarce vertical for the distribution and monetization of music.

As to Point 1 – Lack of adequate supervision to ensure appropriately qualified Expert candidates of ICC were selected and adequately trained.

a) According to the "Selection of Expert Panels" Section 3.4.4 of the new Applicant Guidebook[3], the Objector(s) relied upon specific language that the "panel will consist of appropriately qualified experts (emphasis added) appointed to each proceeding by the designated DRSP." This is also consistent with ICC's language that "the ICC will constitute a pool of qualified candidates (emphasis added) who can be appointed as experts in the new gTLD proceedings.[4]"

The expert appointed to render decisions in EXP_461_ICANN_78 (c EXP_479_ICANN_96 EXP_480_ICANN_97) is not a music, intellectual property, competition regulator or cultural expert versed in the unique music, intellectual property, competition and cultural issues that strongly relate to the music community. The Determinations published on December 9, 2013 (the "Decisions"), demonstrated that the panelist had limited knowledge on the functions of the music community and was ill-prepared to understand and address these unique music community matters.

[3] http://newgtlds.icann.org/en/applicants/agb/objection-procedures-04jun12-en.pdf
[4] http://www.iccwbo.org/Products-and-Services/Arbitration-and-ADR/Expertise/ICANN-New-gTLD-Dispute-Resolution/Experts/

A glance at the Panelist Francisco Orrego Vicuna's qualifications[5] reveal that his specialties are: international law, international trade and investment. ICANN and the ICC failure to select qualified expert candidates (such as experts in competition regulation, intellectual property professors/judges/attorneys, or musicologists, ethnomusicologists, or music industry professors/attorneys), was a breach of the AGB and the obligation to create a meaningful evaluation of community concerns. The panelist, while being an arbitrator, was ill-equipped to address the unique issues presented and the Objectors relied to their detriment on the fact that the ICC would select an appropriate expert to review the Objections. Especially given the significant costs involved, it was reasonable to assume that the appropriate experts would be identified. These failures are evident, as follows:

First, the panelist agreed with Applicant's misleading statement that the music community does not rely on the DNS/Internet, holding that:

> It is thus not possible to conclude that there is in this case a likelihood of concrete or economic damage to the community or that the Applicant intends to act contrary to the interests of such community or interfere with its activities. The dependence of the community on the DNS for its core activities has not been proven (emphasis added)" (Expert Determination, Section 71, p.24)

Any reasonably qualified expert should have taken judicial knowledge of the indisputable fact that the music community is heavily dependent on the DNS for the core of its activities. It is publicly acknowledged and commonly-known that the community most affected and impacted by the DNS was the music community. The DNS has changed the structure of how music (both legal and illegal) is distributed, marketed and consumed (See Annex 2). The DNS has also contributed to massive illegal piracy (e.g. via search engines, P2P networks or sites such as PirateBay) financially harming the community.

Secondly, the panelist lacked qualifications as an expert to render an opinion on whether the Applicant would be anti-competitive, and in his own words, the panelist claimed that competition regulators were the ones qualified to make such a determination:

> Whether there is… anti-competitive behavior…is not something that can be established beforehand and is thus purely speculative... competition regulators will very well know how to address this problem (Section 70, Pg. 25)

[5] http://www.arbitration-icca.org/about/governing-board/MEMBERS/Francisco_Orrego_Vicuna.html

As such, the panelist declined to render an opinion on a key issue of alleged material harm concerning Applicant's exclusive access gTLD policies (an opinion that an appropriately-qualified expert with experience working with competition regulators would have been equipped to render). Similarly, the panelist also ignored Objector's request to review the overall context of the Applicant's strategy to register close over 60+ gTLDs, all of which were closed generic strings, including, not one, but three music related strings, which presents significant anti-competitive concerns and would warrant further investigation as they are likely to create harm to the community and others. Instead, the panelist treated each music-themed gTLD objection in a mutually exclusive manner contrary to how the cases where presented, calling the Objector's reasonable assertion of likelihood of harm with respect to the Applicant's anti-competitive behavior "speculative" (Section 70, Pg. 25). Notably, the GAC Advice, ICANN revisions to the Registry Agreement and the Applicant's own change of position (from exclusive access to open) – pertinent evidence -- was rejected by the panel. Such evidence - if it had been transmitted by ICANN to the ICC for all Community Objection Panelists to consider - would have required panelists to appropriately opine and address as to the merits of such actions.

The panelist also stated that support for pirate networks does not prove harm "that can be established beforehand and is purely speculative" (Section 70, p.24). This statement flies in the face of irrefutable evidence and knowledge that copyright infringement is illegal and it harms the music community's legitimate interests. Such evidence of the Applicant's activity in pirate networks was ignored without reason and referred to as "speculative."

b) The panelist also denied Objector's standing by ignoring the size, composition and breadth of the Related Objector Entities and by failing to consider the standing of an Objector consisting of globally-recognized Label Members and ignoring Associate Members altogether (who have formal membership boundaries with Objector) that cover hundreds of millions of music community members having formal boundaries with Objector's Members. Furthermore the panel disingenuously asserted without any concrete proof or evidence that independent musicians were not strongly associated with the string "music":

> While an association exists of course between the gTLD applied for and the term "music", this is by definition a generic term that might relate to music in general but not specifically to the "independent music community..." (Expert Determination, Section 66, p.24)

Objector Label Members include Labels representing the world’s two best-selling artists of 2012, Adele and Taylor Swift,[6] who are globally recognized and distributed. Associate members, include Apple iTunes (the world’s largest music retailer with majority market share), which formally requires hundreds of millions of music fans to create formal Apple accounts and abide to strict terms of service in order to consume music. This is because objector Associate Members providing legal music (e.g. Apple iTunes or Pandora, the world’s largest music radio) must ensure that royalties are paid to the music community rights-holders using clearly delineated, organized systems that identify rights-holders corresponding to each song sold or streamed (See Annex 3).

It is a fact that nearly all musicians (over 99%) are considered “independent” i.e. not signed to a major label. In fact, “70% of new music being bought is from artists not tied into old industry[7]” (the non-independents referred to as major labels). If one removes independent musicians from the music community then 99% of all music created would not exist. This undeniably proves the panel’s lack of qualifications and incontrovertibly disproves the panelist’s disingenuous assertion that the independent music community is not strongly associated with the “term” music. According to the AGB, “Community” is defined as “meaning “fellowship” – while still implying more of cohesion than a mere commonality of interest.” The Independent Objector reiterates this definition “as a group of individuals who have something in common.” (emphasis added). The common interest universally shared by the community is the “promotion and distribution of music.” Furthermore, ICANN’s definition of “Size” and “Substantial Opposition” relates to “a significant portion of the community[8]” – i.e. not the entire community. Substantial opposition should be taken within “context rather than on absolute numbers[9]” of a substantial portion of the community. The panelist did not follow the AGB language in regards to what constitutes a significant portion and that substantial opposition should be taken in “context rather than absolute numbers” i.e. not requiring “billions” of written expressions. However the panel curiously stated that “with billions of users the expressions of opposition would need to run in high numbers to meet this test.” (Section 63, Pg.23). This clearly showed the panel’s lack of understanding to these proceedings’ rules that “opposition” relates to (i) opposition from the music community, (ii)

[6] International Federation of the Phonographic Industry, http://ifpi.org/content/library/dmr2013.pdf, P.11

[7] http://blog.tunecore.com/2012/02/what-the-riaa-wont-tell-you-tunecores-response-to-the-ny-times-op-ed-by-the-riaa-ceo-cary-h-sherman.html

[8] https://community.icann.org/display/newgtldrg/community+objection+grounds

[9] http://newgtlds.icann.org/en/applicants/agb/string-contention-procedures-04jun12-en.pdf, Module 4-11

not generically by Internet users, and (iii) be taken “within context” not literally. With such an unreasonable and unjustified statement the panel set an impossible threshold for any Objector to meet since using the number “billions” as a reference point to prove “substantial opposition” is irrational, unfair and ensures that any Objector would fail to meet such a standard (emphasis added). In context, in 2012 there were 42,100 employed musicians[10] in the U.S, a country which represents 58% of the global digital music market[11] and 27% of the global music market share.[12] In this context, some Objector U.S Label Members alone represent a significant portion of the global community. As such, denying the Objector standing leads to serious procedural and fairness questions. If the panelist’s statements are taken literally no objector would ever qualify to have their concerns be heard since according to the panelist, **“music” is a generic term and can never have a shared, common interest, nor can a generic term be dependent on the DNS for core activities:**

> A broad community may exist at the generic level… but this is not conducive to the clear delineation envisaged under this standard (Section 60, Pg.21)
>
> While an association exists of course between the gTLD applied for and the term “music”, this is by definition a generic term that might relate to music in general but not specifically to the “independent music community” (66, Pg. 22)
>
> The dependence of the community on the DNS for its core activities has not been proven (Section 71, Pg.24)

These statements run contrary to the Independent Objector who states there are many cases of strictly delineated communities and even filed many new gTLD Community Objections (.charity, .healthcare, .hospital, .indians, .med and .medical)[13] based on his own definition of “community”:

> It can include a community of interests, as well as a particular ethnical, religious, linguistic or similar community… a community can be defined as a group of individuals who have something in common … or a common characteristic … or share common values, interests or goals.[14]

[10] U.S Department of Labor, http://www.bls.gov/oes/current/oes272042.htm

[11] http://www.billboard.com/biz/articles/news/digital-and-mobile/1556590/ifpi-2013-recording-industry-in-numbers-global-revenue

[12] http://www.ifpi.org/content/section_resources/rin/RIN_Contents.html

[13] http://www.independent-objector-newgtlds.org/home/the-independent-objector-s-objections/

[14] http://www.independent-objector-newgtlds.org/home/the-issue-of-closed-generic-gtlds/, Community Objections, Section 3

While “music” is a generic term, it is dependent on a clearly delineated community which shares the common interest of promoting and distributing unique “music” through clearly delineated systems to compensate music community rights holders attributed to each song (emphasis added).

ICANN’s lack of action in ensuring appropriate selection and training of experts created a material harm to Objectors and the community proceedings.

As to Point 2: lack of consideration of the relevance and impact of the GAC Advice on the Community Objection process and failure to advise the ICC and Community Objection Panelists on the GAC Advice.

The Community Objection filing pre-dated the Beijing Communique and raised the same concerns set forth by the GAC and subsequently recognized by ICANN NGPC Resolutions and actions. After the Community Objection proceedings commenced, GAC and ICANN called into question Applications that were filed to run generic gTLDs as exclusive-access registries. This very question was presented by Objector at Objector’s significant expense. ICANN should have either advised the ICC and Panelists or required the ICC and Panelists to review and evaluate the impact and relevance of GAC Advice, Board Resolutions, and Applicant Responses to Category 2 on Exclusive Access, and revisions to the Registry Agreement to address these concerns.

When extremely significant, indeed program wide, issues were raised, the Board should have taken appropriate measures to either: a) suspend the proceedings to avoid further waste of resources addressing Applications that were called into question by GAC Advice; b) ensured that the ICC and Panelists were appropriately advised and educated regarding the importance and effect of the GAC Advice; and/or c) provided clear guidelines to address these issues without harming Objector(s).

As to Point 3: lack of an appeal process for Community Objections thereby denying parties procedures to protect their fundamental rights.

The failure of the Board to address a chorus of voices that called for an appeal mechanism to allow appropriate review of cases has prejudiced Objector’s ability to protect their members’ fundamental and legitimate rights.

ICANN's lack of action forced the parties to: a) bear significant expense; b) detrimentally rely on ICANNs stated policies and procedures for Community Objections; c) led to a breach of process; d) has resulted in Applicants materially changing their positions (e.g. from an exclusive access registry to an open registry) in the middle of a proceeding; and e) resulted in the selection and appointment of an expert that was not prepared to address the unique issues presented.

As a result of the Decisions, the Affected Parties suffered direct financial harm in order to prepare and file the Objections. The Affected Parties will also suffer financial harm, and their members will be globally affected should Applicant ultimately be awarded the most semantic music themed gTLDs, effectively controlling an entire music-related space on the Internet with unclear and unspecified polices, while disallowing the community from their legitimate right to registering their names under a public-resource gTLD.

The Affected Parties suffered a breach of due process in the proceedings because <u>in the middle of the proceeding</u> the Applicant was allowed to seemingly materially change (make a 180-degree shift) their Application from applying to run an exclusive-access registry to accepting GAC Advice on Category 2 Advice to intentionally open its registries. Affected Parties further suffered a breach in the proceedings when the panel, incredulously, <u>refused</u> to evaluate and consider relevant GAC Advice and other pertinent evidence presented.

**7. Describe how others may be adversely affected by the action or inaction, if you believe that this is a concern.**

Other groups adversely affected by the inaction are community applicants who have serious concerns about the unintended consequences and precedents created in the new gTLD Program in relation to Material Changes[15] which are inconsistent to the AGB.

ICANN has opened the floodgates for allowing material changes without any consequences or accountability mechanisms to protect community applicants in a contention set by permitting standard Applicants to submit material changes in their Applications in the form of Public Interest Commitments (PICS) to remedy any faults an Application may have. In context, Community Applications already abide to the Registry Dispute Resolution

[15] http://newgtlds.icann.org/en/applicants/customer-service/change-requests

Procedure (RRDRP) built-in accountability mechanism[16] while standard Applicants do not. Community Applicants also have appropriate restrictions, including policies relating to authentication, Eligibility, Name Selection, Content/Use, and Enforcement to safeguard their communities.

Furthermore, Applicants with exclusive access Applications were also given the opportunity to respond to GAC Category 2 Advice. Nearly all exclusive access Applicants stated their intent to change their Applications to non-exclusive. Such public Responses negatively interfered with Community Objections since objected-to Applicants submitted GAC Category 2 Responses which directly contradict and are contrary to their Community Objection Responses. This is misleading and undermines the credibility of the new gTLD process. Objected-to Applications were given the opportunity to defend their exclusive access position – like they had in the Objection Responses – but decided against it since there are no repercussions for making inconsistent statements or any accountability mechanisms to prevent misleading the panelists. Also other Applicants used PICs – another form of material changes – in their Community Objection Responses which are not in their current Applications. Such changes of position occurring during Community Objection proceedings not found in current Applications indicates the procedural flaws of the Community Objection process and also vindicate Community Objectors' positions. ICANN has even took this issue a step further by revising the new gTLD Registry Agreement during Objection proceedings with language vindicating Objectors views. According to the AGB, any information that is deemed "false or misleading may result in denial of the application."

Such material changes, whether they are ones relating to changing a registry from "exclusive" to "non-exclusive" access or incorporating Public Interest Commitments (PICs) are clear, material changes, because they materially change an Applicant's business model and other critical components in their Application, such as financial statements and their Letter of Credit. Under the ICANN AGB rules such material "changes" will likely "involve additional fees or evaluation in a subsequent application round."

ICANN has introduced and allowed such procedural loopholes which objected-to Applicants have used to circumvent dispute resolution processes and the AGB, while

[16] http://www.icann.org/en/news/public-comment/rrdrp-15feb10-en.htm

Community Applicants with responsible and accountable Applications are not allowed to incorporate such public interest changes to meet the CPE threshold. Loopholes, including Responses to GAC Category 2 advice, PICs or new ICANN NGPC Resolutions materially change Applications, negatively affect contention sets, circumvent Community Objections and create material harm to Objectors and community applicants in a contention set. NGPC Resolutions and ICANN's actions have introduced a harmful precedent to the ICANN new gTLD Program without any repercussions, consistent standards followed or accountability. In some cases, Panels have used NGPC Resolutions, the registry agreement revision and PICs against Objectors to prove that with these new resolutions material harm is avoided. This precedent used is a clear loophole benefiting objected-to Applicants at the Objectors' expense as Applicants argued that accepting GAC advice, new NGPC resolutions, new registry agreement revisions and adding PICs – all material changes – prove there is no possibility of material harm. As such, the existing new gTLD process has lost meaning since any standard Applicant is now allowed to "shift" their position without accountability of any sort or ICANN action to prevent such violations. Furthermore, ICANN is also in the process of once again favoring standard Applicants by giving brands special exemptions.[17]

Furthermore, community applicants and objectors in general have been materially harmed financially and procedurally as the selection of Community Objection experts was inconsistent with the AGB and the published CPE Guidelines which clearly say that experts are "selected based on their knowledge of specific countries, regions and/or industries, as they pertain to Applications.[18] Community applicants have relied on the language of the AGB that experts selected would be appropriately qualified with some credible level of knowledge and expertise on the communities reflected in the Applications determined. In many cases, the ICC has selected Panelists with no clearly appropriate qualifications or credible experience with respect to communities reflected in the Applications determined, which is a clear violation of the AGB, Section 3.4.4 which states that the "panel will consist of appropriately qualified experts." As such, many Objectors were materially harmed by Determinations since Panelists lacked fundamental knowledge of community functions and such precedents might likely harm them in CPE Evaluation.

[17] http://www.icann.org/en/news/public-comment/spec13-06dec13-en.htm

[18] http://newgtlds.icann.org/en/applicants/cpe/guidelines-27sep13-en.pdf, Pg.22

## 8. Detail of Board or Staff Action – Required Information

**Provide the Required Detailed Explanation here:**

On June 19th 2013, a letter was sent to ICANN and the Board which raised serious concerns that **"**the ICC has not identified expert Panelists that have expertise in music - the relevant subject matter of interest for the communities."

On June 24th, 2013 ICANN responded stating that "for the matter of the expertise of the panel members…Section 3.4.4 of the Applicant Guidebook" states:

> 3.4.4 Selection of Expert Panels - A panel will consist of appropriately qualified experts appointed to each proceeding by the designated DRSP. Experts must be independent of the parties to a dispute resolution proceeding. Each DRSP will follow its adopted procedures for requiring such independence; including procedures for challenging and replacing an expert for lack of independence…There will be one expert in proceedings involving a community objection.

ICANN further stated in their response that "ICANN has confidence that the ICC has followed the requirements as expressed by the AGB and has appointed experienced jurists with appropriate qualifications in mediation/arbitration to preside over objection proceedings." However, ICANN's response that the "appropriate qualifications" of an expert is in "mediation/arbitration" is not mentioned in the AGB. The definition of "expert" is "a person who has a comprehensive and authoritative knowledge of or skill in a particular area.[19]" Objectors reasonably relied on the fact that experts would be "appropriately qualified experts" pertaining to the Applications determined and have "comprehensive and authoritative knowledge" in that "particular area."

ICANN's correspondence opens up serious issues of lack of clarity, accountability and transparency in regards to the Community Objection process since the AGB clearly states the word "expert.", not the words "mediator" or "arbitrator" which would have been the appropriate words if ICANN's correspondence statements were applicable. This opens up new questions about the fairness of the process and the high probability of confusion based on the fact that ICANN did refer to the Panelists as "experts" not "arbitrators" or "mediators." This is aligned and consistent with the language used in another community-related

[19] Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/expert

evaluation process where experts are used – the Community Priority Evaluation. Specifically, CPE Guidelines clearly state that "evaluators are selected based on their knowledge of specific countries, regions and/or industries, as they pertain to Applications"[20] which is consistent with the definition of "expert" not an arbitrator or mediator. There is no mention in the AGB that the expert's "appropriate qualifications" would be in "mediation/arbitration" because such qualifications would be inappropriate since they would directly harm Objectors given that Objectors would have the impossible burden of educating unqualified mediators/arbitrators on community specifics, how the community functions and other complexities requiring significantly more words than the maximum permitted in filing.

On July 30th an Additional Submission in light of GAC Advice/NGPC material change Resolutions and clarifications with respect to Amazon misleading Response statements about Objector's standing and material harm was submitted to Panelist:

> Per Ms. Košak's, message of July 30, 2013, we have been directed to confer directly with you. As you may be aware, yesterday we submitted Objector's Request for Leave to File an Additional Submission and Reply to Applicant's Response. Per the attached filing, this submission is made in accordance with Art 17 of the Attachment to Module 3 of the Applicant Guidebook.

On August 20th, the Panelist completely ignored material changes to the Program by GAC Advice, NGPC Resolutions and Applicant misleading statements and rejected the Additional Submission referring to its content as "not exceptional" despite the material changes' influential impact on all new gTLDs and rule changes exceptionally affecting all Applicants:

> Having examined the file... the Expert is of the opinion that it contains all the necessary elements required to reach a Determination on this dispute. Accordingly the Expert considers that there is no need to invite additional submissions as envisaged under Article 17 (a) of the Procedural Rules governing these proceedings. The Expert further notes the Applicant's comment to the effect that under Article 18 of the Procedural Rules production of documents is limited to exceptional cases. No such exceptional case exists at this time. On the basis of these considerations the Request is denied and its contents are not to be included in the file of this case.

In regard to GAC Advice, ICANN solicited responses from applicants for the strings identified by the GAC regarding whether they planned to operate the applied-for TLDs as exclusive access registries (defined as a registry restricted to a single person or entity and/or

[20] http://newgtlds.icann.org/en/applicants/cpe/guidelines-27sep13-en.pdf, Pg.22

that person's or entity's Affiliates" (as defined in Section 2.9c of the Registry Agreement). The responses were submitted to the New gTLD Program Committee (NGPC) of the ICANN Board. On 28 September 2013, the NGPC adopted a Resolution on GAC Category 2 Advice[21] allowing applicants not planning to operate as exclusive access registries, and that are prepared to enter the Registry Agreement as approved, to move forward to contracting.

On October 8th, .MUSIC (DotMusic) sent written correspondence to ICANN[22] in relation to Applicant Responses:

> We write as a follow-up to our most recent Letter to ICANN (October 8th)[23] to formally record and publish our concerns about new material changes arising from ICANN NGPC Resolutions and their impact on the current Community Objection process. Specifically, we would like to highlight the effect of potentially prejudicial "exceptions" through the acceptance of certain GAC advice and ICANN NPGC resolutions.

On October 10th, 2013 .MUSIC followed up its email after the release of GAC Category 2 Advice Form Responses:

> … it has come to our attention that two of the Applicants we have mentioned in our Letter (who are subject to community objections) have materially changed their opinion and clearly stated that their generic string application(s) for music-themed TLDs will no longer be operated as "exclusive" TLDs, a clear statement of admittance that their original applications' "exclusive" access music-themed TLDs create a strong likelihood of harm.
>
> This is exactly the kind of issues on material changes our Letter has been trying to illustrate in light of ongoing Community Objections on the subject matter which now have no other predictable and consistent recourse but to be upheld given the transparent admittance by these Applicants: Amazon,[24] Far Further/ .music LLC.[25] We kindly request these statements by these two Applicants and our Letter be forwarded to the ICC Panelists since they are crucially pertinent to the cases at hand. We also kindly request some clarification statements from both ICANN and the ICC how such material changes will be addressed and handled since these Applicants' community objection responses were inconsistent with these GAC Category 2 Advice statements they have just made. It is clearly evident that (i) their original application submission was not done in error and such material changes and GAC Category 2 Advice statements: (i) affect third-parties materially, especially objectors and applicants in contention set, (ii) create

[21] http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-28sep13-en.htm#2.a
[22] http://www.icann.org/en/news/correspondence/roussos-to-crocker-et-al-08oct13-en.pdf
[23] http://www.icann.org/en/news/correspondence/roussos-to-crocker-et-al-12jul13-en.pdf on the 12th, July 2013 with ICANN response at http://www.icann.org/en/news/correspondence/willett-to-roussos-14aug13-en.pdf on 14th August, 2013
[24] http://newgtlds.icann.org/sites/default/files/applicants/09oct13/gac-advice-response-1-1316-18029-en.pdf
[25] http://newgtlds.icann.org/sites/default/files/applicants/09oct13/gac-advice-response-1-959-51046-en.pdf

> unfairness to both objectors and applicants in contention set, (iii) are material, and (iv), if allowed, create a precedent with unintended consequences to the new gTLD Program.

ICANN responded on October 22nd, 2013.[26] On October 10, 2013 another email was sent to the Expert and the ICC pertaining to Amazon's GAC 2 Response material change and position change in relation to their exclusive access applications for music-themed .music, .song and .tunes alerting GAC of their intentions to change their registries from exclusive to non-exclusive:

> As you may not yet be aware, on October 9, 2013 (yesterday), ICANN published a submission by the Objected-to Applicant that materially affects the instant proceedings. Accordingly, Objector respectfully submits that these statements, and proposed sweeping changes to the Applicant's Applications be considered in connection with the instant matter.
>
> As set forth below, to avoid further conflict with the Beijing Communiqué -- addressing concerns about Category 2 closed generic strings (and the same arguments asserted by Objector and under consideration in the instant proceedings) -- Applicant advised ICANN that it will materially change its position from running the .music, .tunes and .song TLDs as closed exclusive registries to open registries.
>
> Accordingly, the Objector respectfully submits that the instant proceedings must now include an evaluation and consideration of the following ICANN publications dated October 9th, 2013 whereby Applicant states that it will change its Applications from "closed" and "exclusive" to "open."
>
> Through these submissions the Applicant is attempting to circumvent this Objection and other criticism levied against it by "agreeing" to open its exclusive music-themed Registries. See New gTLD GAC Advice: Category 2 Safeguards and Applicant Responses Published October 9, 2013[27] and Applicant's Response to GAC Advice Category 2: Exclusive Access.[28]
>
> These newly-published statements by the Objected-to Applicant (published last night by ICANN) are contrary and inconsistent with the Applicant's Responses to the instant Community Objections. The foregoing submissions establish that the Applicant's originally-exclusionary polices in the objected-to Application(s) are not in the global public interest and would create a certainty of material harm to the legitimate interests of the music community and the global public interest.
>
> Amazon has materially changed its stance with a new statement that their generic string application(s) for music-themed TLDs will no longer be operated as "exclusive" registries even though their current application(s) squarely state that "the TLD(s) will be operated as an exclusive registry." It is evident that Amazon's original position in relation to "exclusive" registry access has changed. Amazon's

[26] http://www.icann.org/en/news/correspondence/willett-to-roussos-22oct13-en.pdf
[27] http://newgtlds.icann.org/en/applicants/gac-advice/cat2-safeguards
[28] http://newgtlds.icann.org/sites/default/files/applicants/09oct13/gac-advice-response-1-1316-18029-en.pdf

> proposed reverse in course is not yet approved and provides new evidence that Objector's concerns - which were raised prior to any public discussion about the harm of closed generics - should be upheld.
>
> On the date that the instant Objections were filed, Applicant's music-themed applications (.music, .song and .tunes) created a certainty of material harm and were against the global public interest. The Applicant's proposed changes to its Applications are not yet approved and final by ICANN and thus the material harm still exists. Therefore, the only remedy is for this Panel to move to protect the community and public interest.
>
> Objector also notes that ICANN's New gTLD Program Committee's (NGPC) Scorecard Resolution No. 10 dated September 28th, 2013[29] pertaining to the "Registry Agreement as approved by the NGPC, prohibits exclusive registry access for generic strings (emphasis added)." Here too, the NGPC resolution "is consistent with the GAC advice." The NGPC has directed ICANN "staff to move forward with the contracting process for applicants for strings identified in the Category 2 Safeguard Advice that are prepared to enter into the Registry Agreement as approved." Essentially, the NGPC and the objected-to Applicant have agreed with Objector's concerns that closed, exclusive registries for .music, .song and .tunes are improper and harmful.
> If an expert determination has already been made that is contrary to upholding the Community Objection against the Applicant, we respectfully request the case be re-opened to address these new contradictory statements by the Applicant and to render a determination that: (i) is consistent with the Applicant's newly published conflicting statements; and (ii) is aligned with GAC advice and ICANN NGPC Resolutions on the issue of exclusive registry access for generic strings.
> Applicant is free to respond to these points and defend its material changes to open these strings in the midst of this Objection.
>
> For the instant Community Objections to have meaning, and this process to maintain integrity, the matter must be re-opened and the issue be submitted for re-evaluation by the Expert.

On October 11, 2013, the Community Objection panelist in relation to Amazon's closed .music, .tunes and .song applications, Francisco Orrego Vicuña, responded:

> I am in receipt of the parties' respective communications dated 10th and 11th October, 2013 in respect of the submission of new information in these cases. The Expert must inform the parties that no such new information can be considered at this stage in the context of the decisions on the cases noted…. under Article 21 of the Dispute Resolution Procedure the Expert is directed to submit its Determination within 45 days of the constitution of the panel. This date has passed…The Objector's request in his communication of 10th October is accordingly not accepted.

[29] http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-28sep13-en.pdf

On November 26th, 2013 the ICC replied to our correspondence and informed in an email that such new information can be considered by the Expert:

> …the Centre has also taken note of the exchange of e-mails between the parties and the Expert with regard to the request for re-opening the case following the Applicant's changes in its Applications. The Centre also notes the Objector's request that the ICC "*review this issue, allow discussion and provide clarification on these points*". The Centre would like to draw your attention to the fact, that the procedure for changing Applications, including the obligation of the Applicant to provide the explanations thereof, is governed by ICANN's rules… please be informed that the decision to re-open the case, should the need arise, and to take into account new or amended documents, is taken by the Expert (emphasis added) based on the information available and nature of the cases in question.

On November 26th, 2013 a response was sent to the ICC and Panelist:

> After carefully reviewing the public Expert Determinations,[30] it is apparently clear that Experts have appropriately used the Applicant Guidebook as a strong reference for their Determinations and rules which makes this issue relevant and procedural in nature. As you have indicated, the procedure for changing Applications is governed by ICANN rules… The Centre also clearly noted that… "the decision to re-open the case, should the need arise, and to take into account new or amended documents, is taken by the Expert based on the information available and the nature of the cases in question.
>
> The rules that the Expert must abide to are governed by ICANN rules and procedures, most notably the language contained in the Applicant Guidebook (AGB). There are specific provisions in regards to Material Changes found in the AGB[31] to which all Applicants – including both Amazon (.music 1-1316-18029, .song 1-1317-53837, .tunes 1-1317-30761) and .music LLC/Far Further (.music 1-959-51046) must abide to, especially if their position is one of "exclusive access." However, they have publicly responded to GAC with a position which is 180 degrees different to their Responses to the ICC and different to their Application. This is misleading, inconsistent and legitimate grounds for concern with respect to procedures. If both Applicants' Responses and "original" Applications were so strong, they did have the option to defend their position with respect to GAC advice - as they did in their Objection Responses - but have now conveniently chosen a different direction, which is misleading and creates a harmful precedent in the ICANN process governing dispute resolution procedures.
>
> It is reasonable to assume that in any proceeding – whether it is one conducted in a court of law or under an ICANN's dispute resolution procedure – that any inconsistencies or changes in position not reflected in the original testimony – the original Application (without any PICs or GAC Advice Category 1 or 2 material

[30] http://www.iccwbo.org/products-and-services/arbitration-and-adr/expertise/icann-new-gtld-dispute-resolution/expert-determination/
[31] http://newgtlds.icann.org/en/applicants/customer-service/change-requests

changes) or their Responses to Objections - should be investigated by the Expert so that the procedures followed by the Expert are compliant with the Applicant Guidebook and no harmful precedent, unintended consequences or loopholes are created.

The ICANN Guidebook's section on "Material Changes" is clear that any information that is deemed "false or misleading may result in denial of the application" (AGB). We strongly believe that many – if not all - music-themed Applicants have provided misleading information in their Responses to the Community Objections because such Responses are not made public by the Centre (emphasis added). As such, there is no Applicant accountability towards the ICANN dispute resolution process or transparency with the Centre since the Applicants' Responses are not made public. We are deeply concerned with misleading music-themed gTLD Applicant Community Objection Responses especially those given to Experts that GAC Advice was "irrelevant." Such statements would not be seen under a positive light by both GAC or the ICANN NGPC if they were made public to them.

It is clear that if an Application is materially changed from "exclusive" to "non-exclusive" (by incorporating Category 2 safeguards) or incorporating Category 1 enhanced safeguards, it will affect its business model, its financial statements and its Letter of Credit. Under the ICANN AGB rules such "changes" will likely "involve additional fees or evaluation in a subsequent application round" (AGB) because the entire premise of the Applicant's Application has changed materially.

Last Thursday at the ICANN Public Forum in Buenos Aires/Argentina, we publicly informed the ICANN Board of these types of procedural loophole concerns which objected-to Applicants can use to circumvent the dispute resolution process. We have also met with the ICANN Ombudsman to express these same concerns and he recommended to reach out to the ICC and the Expert Panelist. The fact that the Centre agrees that "ICANN's new gTLD dispute resolution procedure does not provide for any specific provision in this regard" is clear evidence of procedural loopholes that Objected-to Applicants could use to their benefit to circumvent the Community Objections.

Our objective is that Objections are treated in a transparent and accountable manner, consistent with the Applicant Guidebook and rules contained in the AGB in regards to Material Changes or with respect to a change of position that was not in the original Application. We hope that the Experts acknowledge the issues at hand and the harmful precedent as illustrated in the Material Changes section of the AGB… music-themed gTLD Objectors' arguments, whether on the issue of "exclusive access" or "enhanced safeguards," were based on the Applicant's stated positions found in their Applications… Ultimately, the Expert should rule on the Applicant's stated Policies as found in their Applications taking into consideration any relevant new statements by the Applicant as well as new, pertinent ICANN NGPC Resolutions with respect to "exclusive access" or lack of "enhanced safeguards." Otherwise, the process has no meaning, and as long as a party can "shift" position to avoid scrutiny, there is no accountability.

> Allowing inconsistent statements to be a justification for avoiding an adverse verdict would create a scenario that obviates the need for the Panel in the first place. We agree with the ICANN Resolutions and they provide additional evidence from ICANN - who, as the ICC agrees, writes the Rules - on the obvious harm created by music-themed Applications that do not have “adequate safeguards” or have “exclusive access.” We hope that the Expert Determinations are consistent and do not allow process loopholes for Objected-to Applicants to circumvent the process and the new ICANN NGPC resolutions which have vindicated the concerns presented in the music-themed Community Objections.

On December 3rd, 2013 the ICC responded to our correspondence:

> The Centre carefully considered your comments regarding the above-mentioned case and the provisions of the Procedure and the Rules in this regard. Further, <u>we have communicated your concerns to ICANN</u>. However, at this point the Centre can only proceed pursuant to the current version of the Procedure which does not provide for the possibility of an amendment of the Objection in the course of the proceedings, <u>unless permitted by the Expert</u> (Emphasis Added). Accordingly, <u>it is in his discretion to decide whether to take into account additional submissions</u>...

There is also a lack of clarity with regard to the rules and procedures followed by the ICC and the panelist which are contradictory. On one hand the ICC states that Additional Submissions or amendments due to material changes at any stage of the proceedings can be “<u>permitted by the Expert</u>” and that “<u>it is in his discretion to decide whether to take into account additional submissions</u>”, while on the other hand the Expert denies having this power claiming that “<u>no such new information can be considered at this stage in the context of the decisions on the cases noted</u>” because “under Article 21 of the Dispute Resolution Procedure the Expert is directed to submit its Determination within 45 days of the constitution of the panel.”

It is noted that the ICANN Board and the NGPC responded to the GAC Advice and called for public comment and input regarding “closed generic” Category 2 Applications and took action to materially change how such gTLDs are to be operated and allowed Applicants to intentionally materially change their Applications, in some cases from an exclusive access registry to an open access registry – allowing substantial amendments to Applications <u>during proceedings</u>. During this process ICANN failed to respond to Objector’s stated concerns about the effect of GAC Advice on the proceedings and failed to advise the ICC and panel about the decisions made by ICANN. Moreover, at any point ICANN could have suspended the Community Objection proceedings to allow for a reasoned review and consideration of the impact of such material changes on the wider gTLD process and Community Objections.

**The Affected Parties believe that there was inaction by ICANN:**

1) in failing to adequately train, advise, and instruct the ICC allowing the ICC to appoint an expert who was unqualified to address the specific issues related to music community presented by the Objector. The panel's unfamiliarity with the music community, its cultural composition, its strict delineation and a host of intellectual property issues it faces on the DNS (such as rampant piracy_ as well as the unique impact of the gTLD program on worldwide distribution of music, resulted in a fundamentally flawed decision that is a <u>reversible</u> error (emphasis added);

2) by refusing to present to the ICC and the panelist, GAC-related issues and new NGPC Resolutions: Responses to GAC Advice, Board Resolutions, Changes in Applicant positions through the GAC Advice Category 2: Exclusive Access Response Form for Applicants, and revisions to Registry Agreement that addressed GAC Advice allowed the Objection to proceed <u>without consideration</u> of the effect and importance of these exceptional developments that occurred <u>after</u> the Objections were filed;

3) by <u>allowing a process to facilitate modifications and material changes</u> to Applications are facilitated in response to GAC Advise on Category Exclusive Access Applications permitted Applicant's to <u>fundamentally change positions in the middle of the proceedings</u> without ramifications to the material detriment of Objector;

4) in creating a process by which <u>exceptional modifications and material changes to Applications</u> in response to GAC Advise on Category Exclusive Access Applications can be <u>facilitated</u>. Failing to address the effect of such actions to on-going Objections violated Article 4 of the Articles of Incorporation and Article 1, Section 2, 7, 8, and 9 of the ICANN Bylaws resulting in a breach of process and calls into question the legitimacy of the program; and

5) by <u>failing to offer an appropriate appeal mechanism</u> to address clear procedural issues and AGB violations pertaining to Objections especially in cases of unqualified panels and factually incorrect and inconsistent statements.

6) by harming applicants in a contention set as well as Community and Legal Rights Objectors against Amazon for the same strings that relied on the AGB's language. Amazon's position change in regards to exclusive-access, affects both Community Objections and Legal Rights Objections since they vindicate Objectors' arguments on the material harm test.

7) in failing to ensure there were no conflicts of interest and bias in panels relating to the new gTLD Objection process as whole. The Applicant's general counsel Doug Isenberg representing Amazon in these new gTLD Community Objections was also a Panelist determining a decision against another Objector (Food Network) in a new gTLD Legal Rights Objection proceeding. DotMusic has been involved in both Community Objections and Legal Rights Objections against Applicant for the same objected-to music-themed strings and such panel selection conflicts violate the AGB and introduces unintended precedents in that other panels may rely on for their determination. This compromises the credibility of the new gTLD program and sheds light on how Objections were mishandled by ICANN without any accountability on the selection of panels even if there was a clear conflict of interest.

**9. What are you asking ICANN to do now?**

The Affected Parties respectfully request that ICANN:

1) Reimburse or order the ICC to reimburse the Objector for all of its expenses, including but not limited to attorney fees, administrative expenses and Expert fees associated with cases: EXP_461_ICANN_78 (c EXP_479_ICANN_96 EXP_480_ICANN_97); and

2) Allow for new Community Objections to be filed for these Applications with the appointment of an appropriate Expert (noted as an expert in music/intellectual property/competition regulation);

3) Determine that Applicants that have made public statements intending to substantially amend their Applications by responding to GAC Advice be deemed material and inconsistent with their position in Community Objection Responses and rule in favor of Objectors given that it is admission of their harmful policies; or

4) Allow for a Reconsideration of the Decisions by an appropriate and qualified expert and with instruction regarding the GAC Advice and changes made by Applicants

**10. Please state specifically the grounds under which you have the standing and the right to assert this Request for Reconsideration, and the grounds or justifications that support your request.**

DotMusic Limited (.MUSIC) is a new gTLD Applicant for the .music music-themed community application. The new gTLD Applicant and Objector(s)/Related-Objector Entities are entitled to a fair and appropriate evaluation of the AGB policies and procedures. Moreover, DotMusic as a competing applicant is adversely affected by ICANNs granting of modifications and changes to Applications in response to GAC Advice on Category 2 Exclusive Access Applications publicly stating Applicant's intention to fundamentally amend Applications and change positions without consideration on how such action affected other Applicants or the Community Objection process.

Furthermore, such panel decisions and false statements not based on facts pertaining to Objector's standing as a clearly delineated community (See Annex 3) or the music community's dependence on the DNS for activities (See Annex 2) can adversely affect the Community Priority Evaluation (and DotMusic as a community applicant) since EIU Evaluators could use the expert's factually incorrect opinion as precedent and fail Community Applicants in general (emphasis). DotMusic has spent over 8 years, significant resources and millions of dollars building the .music brand and receiving support from a significant portion of the community to pass CPE. If CPE fails, DotMusic will be subject to expensive auctions which were designed to favor deep pocketed standard Applicants – such as Amazon and Google – not community applicants.

The Objector and Related Objector Entities were entitled to a fair and appropriate management of the Objection proceedings in accordance with the AGB. By providing inadequate training and guidance to the ICC, ICANN allowed the ICC to appoint an unqualified expert that resulted in fundamentally flawed proceedings, factually incorrect statements and a harmful determination which creates a harmful precedent.

### Breach of Fundamental Fairness

Basic principles of due process to the proceeding were violated and lacked accountability by ICANN, the ICC and the Panel. ICANN failed to consider concerns about the selection of the panel and the ICC failed to follow the procedures the AGB set in relation to selecting an appropriately qualified expert in the subject-matter reflecting the Applications despite the excessive costs and resources attributed to filing. The panel also selected not to hear legitimate concerns and striking evidence by the Objector which were crucially relevant even contradicting the ICC's clear statements that it was up to panel's discretion to do so.

Failure to Consider Evidence

The Panel failed to consider relevant evidence relating to: (i) The Applicant deciding not to defend their exclusive access position and making a complete position change in their GAC Category 2 Response public statements changing from exclusive-access to non-exclusive, proving that their current Application creates a likelihood of material harm leading to a ruling favoring Objector; (ii) The clear standing of Objector as a clearly, delineated community; (iii) The significant size and global breadth of the Objector Members; (iv) How the music community is dependent on DNS/Internet for core activities.

Violation of ICANN Articles of Incorporation

Article 4 calls for ICANN to operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law, and to the extent appropriate and consistent with its Articles and Bylaws, through open and transparent processes that enable *competition and open entry in Internet related markets.*

ICANN should have properly communicated and delegated functions to the ICC and failed to do so in violation of ByLaws Art. 1, Section 2, 3 *To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties*.

ICANN or the NGPC should have properly communicated to the ICC and the Panelists the existence and effect of GAC Advice, PICs, NGPC Resolutions and Registry Agreement revisions on pending Objections. ICANN or the NGPC should have also considered the effect of allowing such substantial amendments to Applications and material changes to the gTLD Program (ByLaws Art. 1, Section 2, 7 *Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most affected can assist in the policy development* *process*; ByLaws Art. 1, Section 2, 8 *Making decisions by applying documented policies neutrally and objectively, with integrity and fairness*.

Between April, 2013 and December 9, 2013 (the date of the Decision), ICANN could have acted to protect Applicants and Objector from material harm by properly addressing material flaws with the ICC Process and/or informing the ICC and Panelists regarding the GAC Advice and related issues (ByLaws Art. 1, Section 2, 9 *Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most affected*; ByLaws Art. 1, Section 2, 10 *Remaining accountable to the Internet community through mechanisms that enhance ICANN's effectiveness*; ByLaws Art. 1, Section 2, 11 *While remaining rooted in the private sector, recognizing that governments and public authorities are responsible for public policy and duly taking into account governments' or public authorities' recommendations*; and ByLaws Art. 3, Section 1 *ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness*.

**11. Are you bringing this Reconsideration Request on behalf of multiple persons or entities?**

X Yes

**11a. If yes, Is the causal connection between the circumstances of the Reconsideration Request and the harm the same for all of the complaining parties?**

Yes, because the music community (i) has a shared, common interest - the legal distribution and promotion of music, (ii) is dependent on the DNS (where rampant piracy occurs) for core activities, and since (iii) Determinations of such significance pertaining to competition and exclusive access can create material detriment to the legitimate interests of a significant portion of the music community that is represented by the Affected parties. Failure of the panelist to understand that the music community is reliant on the DNS exhibits why this particular case requires someone familiar with music/intellectual property matters.

**Do you have any documents you want to provide to ICANN?**

Yes, please see Annex. Attached are the (i) 3 Expert Determinations for .music, .song, and .tunes (See Annex 1), (ii) Proof of evidence that the music community is reliant on the DNS/Internet for core activities (See Annex 2), and (iii) Proof of evidence that the music community is clearly and strictly delineated (See Annex 3), which was mentioned in the Additional Submission.

**Terms and Conditions for Submission of Reconsideration Requests**

The Board Governance Committee has the ability to consolidate the consideration of Reconsideration Requests if the issues stated within are sufficiently similar. The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious. Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing. The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC. The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.

______________________________ 12/22/2013

Constantinos Roussos Date

DotMusic (.MUSIC)

# Appendix C

.MUSIC (DotMusic Limited) Reconsideration Request Against Community Objection Decisions Relating to Music-Themed  Applications with Exclusive Access Language or Lack of Enhanced Safeguards

**1. Requester Information**

**Name: Constantinos Roussos**

Contact Information Redacted

**Address:**

**Email:** Contact n ormation Redacted **with a copy to counsel,** Contact Information Redacted

**2. Request for Reconsideration of:_X_ Staff action/inaction**

**3. Description of specific action you are seeking to have reconsidered.**

DotMusic is challenging ICANN's inaction on 5 issues:

1) In not properly supervising and ensuring that selected Expert candidates of the ICC (i) were appropriately qualified and knowledgeable about core subject matter to correctly apply standards for determining existence of a substantial clearly delineated community invoked which was expressing opposition; (ii) had no direct or indirect conflicts of interest; (iii) were adequately trained and informed to address unique issues presented by Community Objections and gTLD Program including material changes in AGB. The community expected that the ICC would be required to appoint and advise an appropriately qualified "expert," (not just an arbitrator) familiar with the unique needs and requirements presented in the gTLD Program, intellectual property and anti-competitive issues, and the needs and composition of the relevant community (i.e. a music expert for music-themed Objections) (Point 1);

2) In not recognizing the relevance and impact of the exceptional GAC Advice on Community Objection process, and not advising the ICC and Community Objection Experts on effects of new binding contractual material changes in the Program arising from GAC Toronto and Beijing Communique and subsequent GAC Advice: PICs, GAC Category 1 Enhanced Safeguards, Responses to GAC Advice, Board Resolutions, Applicant position Material Changes through their GAC Advice Category 2 Exclusive Access Responses, and revisions to the new gTLD Registry Agreement[1] (the "Material Changes") These addressed GAC Concerns pertaining to exclusive access which were directly related to anti-competitive and enhanced safeguard issues (the "Safeguards") raised in Community Objections. (Point 2);

3) In not creating an appropriate appeal process for Community Objections and denying parties

[1] 3(c) and 3(d) of Specification 11 provided that: (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" [. . .]. "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 (New gTLD Registry Agreement, July 2nd, 2013, https://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm#1.d).

procedures to protect their fundamental rights and legitimate interests, including preventing conflicts of interest, determinations based on applying contradictory standards and on false facts (Point 3).

4) ICANN (i) giving preferential treatment to .brand Applicants and all Applicants without Safeguards in their current applications. ICANN put in motion a process for Applicants to make material changes to their Applications in the form of PICs[2] and changes in Specification 13.[3] This materially undermines the Legal Rights and Community Objection process, contention set neutrality and Applicant equal treatment, and (ii) giving preferential treatment to the String Confusion Objection process to introduce a review mechanism to address perceived inconsistent Expert Determinations limited to Determinations made on String Confusion objections for .CAR/.CARS and .CAM/.COM.[4] Perceived inconsistent decisions in Community Objection process were not given same type of treatment (Point 4).

5) With respect to GAC Category 2 Advice Response, ICANN did not verify whether some Applications had exclusive access language. This allowed Applicants (e.g. .music LLC, 1-959-51046 – Annex J) to circumvent the change request requirement initiated by ICANN if objected-to Application (such as in the case of Amazon's .music, .song and .tunes Applications which have to file change requests) contained exclusive access language if disclosed in Applicants' GAC Response.[5] In cases of a clear discrepancy between what the Application states and what the objected-to Applicant provided in their Response, ICANN did not taken any action to ensure that these Applicants are required to submit a change request because the Registry Agreement provides that registry operators 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" (2.9(c) of Registry Agreement).

**4. Date of action/inaction:** Determinations were published on February 18th, 2014 (Annex A).

**5. On what date did you became aware of action or that action would not be taken?** 2/18/2014

**6. Describe how you believe you are materially affected by the action or inaction:**

ICANNs acceptance of the Expert Determination will allow .MUSIC and .BAND Applicants to proceed to delegation with policies that are unclear and undocumented. The Expert's determination is based on incorrect standards and incorrect information regarding standing of the Objector and the relevance (or in the Expert's determination, the lack thereof) of the GAC Advice. These two critical errors resulted in a flawed decision on Objectors' standing, and allowed the Expert to "avoid" evaluating

[2] http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm
[3] http://www.icann.org/en/news/public-comment/spec13-06dec13-en htm
[4] http://www.icann.org/en/news/public-comment/sco-framework-principles-11feb14-en htm
[5] http://newgtlds.icann.org/en/announcements-and-media/announcement-4-09oct13-en

and determining whether or not the stated Applications created material harm or whether they protected the interests of the affected community.  The appropriate standard for standing was applied by other Experts in the case of sensitive strings such as .bank, .insurance, .sport, .sports .bank, .charity and .med (Applications which lacked Safeguards) and against exclusive access registries (such as .polo) with findings of material harm. All these Objections were upheld.[6] (emphasis added)

DotMusic (".MUSIC") represented Objectors/Related-Objector Entities in Community Objections constituting clearly-delineated community invoked. The Objector American Association of Independent Music ("A2IM") represented its Members (both Labels and Associates), the U.S. Independent label music community and global independent music coalition. These clearly delineated community of established institutions expressing opposition – as evidenced by a public letter to ICANN[7] by A2IM Coalition - included: Merlin (a global rights agency for the independent label sector, representing over 20,000 labels from 39 countries focusing purely on the interests of the global independent music sector, pg.8), Worldwide Independent Network (representing label creators in over 20 countries), Association of Independent Music (representing companies from largest and most respected labels in the world, Pg.6), and IMPALA (Independent Music Companies Association on behalf of over 4,000 independent music companies and national associations across Europe representing 99% of micro, small and medium sized music actors," Pg.7), who collectively constitute a majority of the independent music community globally invoked (emphasis added) to which strings are explicitly or implicitly targeted. Members of Objector, the International Federation of Arts Councils and Culture Agencies ("IFACCA"), include arts councils and government agencies (ministries of culture) from nearly 70 countries ("Affected Parties"). Both Objectors expressing opposition are clearly delineated and strongly associated with music-themed strings.

On 13th March, 2014, Objections (EXP/462/ICANN/79 (c. EXP/463/ICANN/80, EXP/467/ICANN/84, EXP/470/ICANN/87 EXP/477/ICANN/94), ICC EXP/474/ICANN/91, ICC EXP/459/ICANN/76, ICC EXP/460/ICANN/77) were filed against music-themed Applicants with (i) "open" .music and .band strings without enhanced safeguards to prevent abuse, piracy and protect copyright and intellectual property; or (ii) a discriminatory, anti-competitive exclusive-access registry for .music (the "Objections") each of which were denied.

As to Point 1 – According to "Selection of Expert Panels" Section 3.4.4 of the new Applicant Guidebook[8], the Objector(s) relied that the "panel will consist of appropriately qualified experts

[6] http://www.iccwbo.org/products-and-services/arbitration-and-adr/expertise/icann-new-gtld-dispute-resolution/expert-determination/
[7] http://www.icann.org/en/news/correspondence/bengloff-to-crocker-et-al-06mar13-en.pdf
[8] http://newgtlds.icann.org/en/applicants/agb/objection-procedures-04jun12-en.pdf

(emphasis added) appointed to each proceeding by the designated DRSP," consistent with ICC's language that "the ICC will constitute a pool of qualified candidates (emphasis added) who can be appointed as experts in the new gTLD proceedings."[9]

The Determinations (the "Decisions"), demonstrated that Expert had limited  on functions of the substantial clearly delineated community invoked and was ill-prepared to understand and address these unique issues by applying correct standards for standing.

The Expert's qualifications[10] reveal that, while a noted and highly respected expert, he is not an expert on music. None of the Expert's nearly 50 publicly-listed publications focused on music-related issues or concerns.  It also has come to the Objector(s) attention that there have been public comments regarding potential conflicts of interest concerning the Expert and his relationship with Samsung. See e.g. ("U.K judge who issued extreme ruling for Samsung against Apple hired by Samsung"[11] and "Conflicts of interest are just classier with English accents"[12]). Further, U.S Government documents reveal Expert worked for Samsung (Annex K) after Panelist ruled in favor of Samsung against Apple in a patent case he was the Judge.  Here, Google, an objected-to Applicant, is Samsung's multi-billion dollar strategic business partner.[13] Google's Android has a 79% global market share[14] with Samsung devices dominating 63% of those Android phones.[15] Accordingly, there is a potential appearance of bias (with respect to Google) and ICANN and the ICC accordingly did not retain qualified expert candidates without potential conflicts of interest or those having the relevant experience or expertise to address the unique issues presented by the cases.

Other concerns include, firstly, Expert's determination that Objectors had no standing in contradiction to AGB. The Expert's rationale was whether "music" or "band" is a clearly delineated community covering all of mankind. **That is contrary to AGB standards which are whether the community invoked by the Objector(s) is a clearly delineated community (3.5.4)**. Expert's rationale was also inconsistent with Board Governance Committee's .CHARITY Re-consideration Decision:[16]

> The issue is not whether the term "charity" defines a clearly delineated community. The issue, as set forth in the Guidebook, is whether the community invoked by the objector is a clearly delineated community. ...the Panel correctly applied the standards for determining whether the community invoked by the IO was a

[9] http://www.iccwbo.org/Products-and-Services/Arbitration-and-ADR/Expertise/ICANN-New-gTLD-Dispute-Resolution/Experts/
[10] http://www.ucl.ac.uk/laws/academics/profiles/index.shtml?jacob
[11] http://www.fosspatents.com/2013/02/uk-judge-who-issued-extreme-ruling-for html
[12] http://abovethelaw.com/2013/03/conflicts-of-interest-are-just-classier-with-english-accents/
[13] http://www.pocket-lint.com/news/126816-samsung-and-google-sign-big-ten-year-patent-partnership
[14] http://www.prnewswire.com/news-releases/strategy-analytics-android-captures-79-percent-share-of-global-smartphone-shipments-in-2013-242563381.html
[15] http://www.localytics.com/blog/2013/fonblets-and-phablets-samsung-has-share-of-android-mobile-devices/
[16] http://www.icann.org/en/groups/board/governance/reconsideration/14-3/determination-corn-lake-27feb14-en.pdf, Pg.7

> clearly delineated community. (Determination ¶116, Pg. 2)

Secondly, the Expert agreed with misleading and plainly erroneous statements made by objected-to Applicants **that "GAC Advice was irrelevant" which undermined GAC Advice's critical relevance to the new gTLD Program despite the Objector(s) Additional Submission** (Annex B). Despite our correspondence, the Expert determined that ICANN did not take "any action" on GAC Advice (despite ICANN agreeing on a process to implement new material binding contractual amendments to "fix" Safeguard issues presented by Objectors) and that GAC Advice was "irrelevant":

> What difference does it make?... Nor has ICANN yet taken any action on the advice. (e.g EXP/462/ICANN/79 Determination, ¶18, Pg. 7)… I accordingly hold that the GAC Advice is irrelevant to what I have to decide (e.g EXP/462/ICANN/79 Determination, ¶20, Pg. 7)

In a letter to GAC,[17] the ICANN reiterated the exceptional relevancy of GAC Advice to the new gTLD Program as a "binding contractual obligation" for Applicants:

> By implementing the GAC advice as a contractual obligation in the PIC Specification, the GAC's advice (as implemented) has the weight of a binding contractual obligation.

As to Point 2: The Community Objection(s) filing pre-dated the Beijing Communique and raised the same concerns set forth by the GAC and subsequently agreed upon by ICANN NGPC Resolutions. After the Community Objection proceedings commenced, GAC and ICANN called into question "open" Applications that lacked enhanced safeguards for sensitive music-themed strings and an Application filed to run a generic music-themed gTLD as exclusive-access registry. This very question was presented by Objector at Objector's significant expense. I**CANN should have taken appropriate measures to either: a) align the proceedings with GAC Advice and NGPC Resolutions in a consistent manner to accurately reflect new contracting provisions without harming Objector(s) whose concerns were aligned with Advice/Resolutions; b) ensure that the ICC and Experts were appropriately advised on the relevancy of GAC Advice/Resolutions and new AGB material changes in contracting.**

The AGB states that the "receipt of GAC advice will not toll the processing of any application (i.e., an application will not be suspended but will continue through the stages of the application process)." (Guidebook, Section 3.1.) The Objectors did not ask to suspend the processing of the Objections but rather for ICANN to communicate such critical GAC Advice that was exceptional and agreed upon by the NGPC in those cases that such advice imitated both the opinion of GAC and ICANN and Objectors. It would be grossly unfair for ICANN to work towards implementing GAC Advice and new material contracting provisions to "fix" the same concerns expressed by the Objectors (i.e. giving the

[17] http://www.icann.org/en/news/correspondence/crocker-to-dryden-10feb14-en.pdf , Attachment B, Pg.7

opportunity for objected-to applicants to submit material change PICs to circumvent Objections after seeing every other competitor's publicly-available Application to "repair" and "fine-tune" their Application's lack of safeguards to protect the public interest). As per AGB material changes[18] provisions, it is such new material contractual changes for Applicants would be construed as material changes harming Objectors, 3rd-parties and Community Applicants who already had such safeguards in their Application. If such new amendments are implemented by ICANN as contractual obligations, immediately ICANN is liable for "material changes" harming 3rd-parties and Objectors, especially if those provisions were implemented to protect the public interest from the same concerns that were expressed by the Objectors in Objections that were dismissed (emphasis added). If the objected-to Applications were not going to cause a "likelihood of material" harm then why did ICANN agree to GAC Advice and to implement contractual provisions focusing on preventing the same harms expressed in Objections?

As to Point 3: Expert did not apply the AGB Rules on "standing" and relied on misleading and clearly erroneous statements in his Determinations' rationale, despite Objector submitting clarifying letters and Additional Submissions to both the ICC and the Expert (Annex B, E, J, L).

AGB states that "established institutions associated with clearly delineated communities are eligible to file a community objection" and that the "community is strongly associated with the applied-for gTLD string" (3.2.2.4). In all cases the Expert agreed that Objectors were both "established institutions":

> To my mind A2IM is, on balance to be regarded as established" and "would be fanciful to hold that A2IM has no recognition whatever outside the U.S (e.g EXP/477/ICANN/94, Determination, ¶28, 9). "IFACCA is an established institution, I need not consider this point further" (e.g EXP/474/ICANN/91, ¶23, 7)

However, the Expert ignored the AGB and applied a contradictory test for standing focusing on whether the term defines a clearly delineated community not the Objectors. The issue, as set forth in the Guidebook, is whether the community invoked by the objector is a clearly delineated community (ICANN Board Governance Board, .CHARITY Re-Consideration). In contrast, the Expert incorrectly focused on the string as a generic word and a general "mankind" community, not the community invoked by the Objectors, creating a standard that can never be met since it is impossible to receive letters of support or opposition from all of "mankind" and use "mankind" as a standard for "strong association":

> Music appeals to nearly all mankind… Just because there is one word covering all kinds of music does not make all mankind into a "music community" – the word will not stretch that far. There is no cohesion or relationship between all those concerned with creating, performing, recording or "consuming" music of all the different sorts known to man (e.g EXP/477/ICANN/94, ¶29, Pg. 9)

[18] http://newgtlds.icann.org/en/applicants/customer-service/change-requests

Further, the Expert acknowledged that he did not test whether the community invoked is a clearly delineated community or have an implicit/explicit interest in strings and determines that the only established institution eligible for standing has to "amount to a global music community for all mankind" not the "independent music community" or "ministries of culture governments and arts councils":

> If you took them all (Objector's invoked clearly delineated community) as being a "community" (which I do not) they could only form a part of the global citizenry (all of mankind) which has an interest of any sort in music"…The Objectors "membership (even taken as a whole) cannot in any way be taken to amount to a global music community for all mankind (e.g EXP/477/ICANN/94, ¶30, P.10)

Also the Expert did not apply the standard for a clearly delineated community invoked by the Objector. In contradiction to the AGB he applied it in a generic sense:

> The same generic word covers all music. But a generic word does not itself evidence anything which can be fairly be called a "community" even in the widest sense of the word. There is no public recognition of a music community locally or globally" (EXP/474/ICANN/91, ¶30, Pg. 9).

The AGB standard for standing is not to determine whether the generic term "band" or "music" is a community. As the Board Governance Committee pointed out in other determinations (e.g .gold and .charity), the test is not to determine whether a term is a community but to determine whether the established institution invoked expressing opposition is a clearly delineated community, is substantial and if it has a strong association with the string regardless whether targeting is direct (explicit) or indirect (implicit) i.e. not the Expert's incorrect standard used that allowed the Expert to rationalize that "because a group of musicians may be called a "band" does not mean it forms anything which can be fairly be called a "community" of bands (EXP/460/ICANN/77, ¶32, Pg. 11). A "community of bands" is not the standard that must be proven. The Expert repeats this standard incorrectly:

> Can all carious disparate types of groups of performers around the world who might fall with the description "band" be described as a community? I think not. Just because a group of musicians may be called a "band" does not mean it forms part of anything which can be fairly called a "community" of bands. (EXP/459/ICANN/76, ¶31, Pg. 9).

On one hand the Expert acknowledges that the ".band string is explicitly or implicitly targeted at groups of musicians" and that Objector's "members doubtless have an interest in the bands signed to them" but on the other hand uses the incorrect standard by stating that Objector's "members are not themselves bands at all" and "that the interest is only indirect" (EXP/460/ICANN/77, ¶33, Pg. 11). The test is not to determine whether members of the established institution are "bands" or "music" or that an "indirect interest" in a "band" or "music" themed-string has no weight (in fact, "implicit" (or indirect) targeting is acceptable under the AGB). The appropriate test is whether the established institution has a strong association with the music-themed strings "band" or "music" regardless whether the targeting is explicit or implicit (emphasis added). According to the AGB, the standard is 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" (AGB, 3.5.4) i.e. targeting "may be explicitly (directly) or implicitly (indirectly) targeted." (emphasis added). According to the AGB, the Objectors did not have to prove the incorrect standard assumed by the Expert which was:

> It is not proved that there is such a thing as a community of bands or that A2IM is "associated" with any bands, still less with a "clearly delineated community" of bands (EXP/459/ICANN/76, ¶35, Pg. 9).

The Expert disregarded the community invoked by Objectors and applied a test that no established institution can ever meet: "The community is effectively humankind" (EXP/474/ICANN/91, ¶31, Pg. 9).

Just as in the case of .sport and .charity, the Board Governance Committee correctly applied the correct standard for standing in the .gold Re-Consideration Request determination:

> World Gold Council's community objection, however, refers to the gold industry in general and not to the gold mining industry in particular." (Id.) And as stated in the Guidebook, for a Community Objection to be successful, the objector must prove, among other "the community invoked by the objector is a clearly delineated community." (Guidebook, §3.5.4; see also id. ("The objector must prove that the community expressing opposition can be regarded as a clearly delineated community") (emphasis added)

Here, Objectors and their memberships and affiliations expressing opposition did not invoke the objection on behalf of the "global music community" or "all of mankind." The Objectors' clearly delineated community invoked that was expressing opposition did not describe itself as a being a "community" which was a "part of the global citizenry (all of mankind)." **The expressed opposition was on behalf of the independent music community (A2IM) and a federation of nearly 70 governments' ministries of culture and arts councils (IFACCA). The clearly delineated membership of independent music community brought forward is the globally largest and most influential of its kind e.g. A2IM alone (not including IMPALA, Merlin, WIN, AIM and others which expressed opposition – emphasis added) collected 50% of all the Grammy Awards, the most globally-recognized music awards** (Annex H). Furthermore, the clearly delineated "ministries of culture governments and arts councils" invoked also constitute substantial opposition. Both are strongly associated with strings and critical to the global, legal promotion and distribution of music (emphasis added).

Despite agreeing that both Objectors are "established institutions" the Expert refused to find that Objectors act as "spokesperson[s] for [their] members." This finding was made despite the Expert acknowledging both Objectors' Mission Statements (e.g Objector statements that it "will represent the Independent sector's interests" (EXP/474/ICANN/79, ¶13, P.4 and P.5), The Expert also questioned the Objectors' authority to represent members despite acknowledging that Objectors received letters of Objection support from their corresponding Board of Directors, including Objection support from

Related-Objectors constituting the community invoked. The Expert also failed to consider evidence that both Objectors publicly and privately alerted their Board and all members in newsletters, even posting Objection details publicly.[19] Not a single member expressed disagreement with Objectors' actions.

No other Expert in the ICC Community Objection proceedings required letters from individual members of an established institution that was objecting except this Expert:

> Although it exhibits letters of support from some of its members, there are none at all from any actual band or its manager (e.g EXP/459/ICANN/76, ¶32, Pg. 9)

Just in the case of Community Priority Evaluation (CPE),[20] letters from individuals that are not established institutions have no weight with Community Objections. The AGB has no inference of requesting letters from individual members that were not considered established institutions (emphasis added). We communicated this fact with the ICC and the Panel in writing (before and during the proceedings) and even alerted the Expert that if such letters were material we would provide them (Annex E). The ICC correctly agreed that the Rules did not have any language asking Objector Related Entities / individual members to send letters to the Expert (Annex L).

The Expert also improperly stated that Objectors did not have sufficient association with their own invoked community and membership and discredited DotMusic's associate membership with IFACCA, including DotMusic' s supporting membership:

> I conclude that A2IM does not have any sufficient association with the invoked community." (e.g EXP/477/ICANN/94, ¶38, Pg. 11) …IFACCA can not get its own standing by piggybacking members (EXP/474/ICANN/91,¶25, Pg. 8)

In context, governments that comprise GAC are strongly associated to government Ministries of Culture which are members of IFACCA. In fact, the governments are the same (they just constitute different Ministries within the government). Both the position of IFACCA and GAC on Safeguards are the same with no opposition to such positions. If "government culture ministries" have no standing (or a strong association with music-themed, cultural strings), then GAC should have no standing to object either (This is not true per the AGB).

The Expert also relied on false information for determining "Substantial Opposition":

> Only 18 label members wrote supporting letters. They are of course a much smaller proportion of the world indie population and still less of the world record company industry. They do not amount to a significant portion of the community targeted. (EXP/477/ICANN/94, ¶42, Pg. 12).

[19] http://a2im.org/2013/02/04/call-to-action-please-write-icaan-about-how-music-should-be-administered/ and http://www.a2im.org/downloads/Music_US_Objection_Letter_Template.pdf and http://www.ifacca.org/announcements/2013/02/27/express-your-view-applications-new-music-domain/

[20] http://newgtlds.icann.org/en/applicants/cpe/guidelines-27sep13-en.pdf

In contradiction to what Expert alleges, the letters submitted constituted the entire Board of the Objector, not individual members. The letters (Annex C) also represent Objector's Coalition of globally-established institutions representing clearly delineated significant portion of independent music community invoked that is strongly associated with the strings. These established institutions – as evidenced by a letter[21] by the A2IM Coalition sent to ICANN - included Merlin (global rights agency for the independent label sector, representing over 20,000 labels from 39 countries focusing purely on interests of global independent music sector, pg.8), Worldwide Independent Network (representing label creators in over 20 countries), Association of Independent Music (representing largest and most respected labels in the world, Pg.6), and IMPALA (Independent Music Companies Association on behalf of over 4,000 independent music companies and national associations across Europe, representing 99% of music actors in Europe which are micro, small and medium sized enterprises," Pg.7).

For the Expert to inconsistently conclude "that the Objector's members form a very minor proportion of the world's record companies" (EXP/463/ICANN/80, ¶34, 10) and that such Objections hold no standing or that the community invoked has no relationship to the applied-for string is ill-conceived. The Expert even acknowledged that the Objector has "131 Associate Members, some of whom are large and well-known such as Spotify and iTunes." (EXP/462/ICANN/79, ¶15, 6) is in contrast to his view that the community invoked is not substantial." A member such as iTunes Apple iTunes,[22] another example of "clear membership" with "formal boundaries, geographic reach and size"[23] is substantial. The Objector's memberships cover a global reach and are strongly associated with strings e.g. iTunes accounts for 63% of global digital music market[24] – a majority - with 575 million active global members[25] who have downloaded 25 billion songs from iTunes' catalog of over 26 million songs, available in 119 countries. Other members include Pandora (72.4m active users), Spotify (6m paid subscribers, 24 million active users in 35 countries). A2IM members also include entities associated with global governments, such as France (BureauExport[26]), China (China Audio Video Association[27]) and Germany (Initiative Musik).[28] These three members alone (together with U.S market) represent substantial music economies and a significant portion of community invoked. In context, in 2012 there were 42,100 employed

[21] http://www.icann.org/en/news/correspondence/bengloff-to-crocker-et-al-06mar13-en.pdf
[22] http://a2im.org/groups/itunes
[23] http://www.apple.com/legal/internet-services/itunes/ww/index.html
[24] http://appleinsider.com/articles/13/04/16/apples-itunes-rules-digital-music-market-with-63-share
[25] http://appleinsider.com/articles/13/06/14/apple-now-adding-500000-new-itunes-accounts-per-day
[26] http://a2im.org/groups/french-music-export-office
[27] http://a2im.org/groups/china-audio-video-association-cava
[28] http://a2im.org/groups/initiative-musik-gmbh

musicians[29] in the U.S, a country representing 58% of the global digital music market[30] and 27% of global music market share. “Size” and “Substantial Opposition” relates to “a significant portion of the community[31]” invoked – i.e. not entire mankind. AGB states “Substantial” should be taken within “context rather than on absolute numbers.”[32] As mentioned in Objections and Additional Submissions (Annex B), Objector is strongly associated with strings and community invoked,[33] the Coalition for Online Accountability,[34] MusicUnited,[35], MusicFirst,[36] Copyright Alliance.[37]

The Objector’s participation and recognition by the U.S Government as an important advocate for international music trade activities[38] also counters Expert’s incorrect conclusions that providing further support that the Expert did not apply the correct standard and failed to accurately balance factors for standing. Standing factors were not balanced by the Expert, included a “presence of mechanisms for participation in activities, membership and leadership” (i.e. both Objectors had strict membership and a formal Board of Directors with voting rights), “an institutional purpose related to the benefit of the associated community” (i.e. both Objections had a public and clear Mission Statement and Purpose), “performance of regular activities that benefit the associated community” (i.e. both Objectors had Outreach and events) and “level of formal boundaries around the community” (i.e. both Objectors required members to formally apply to become members with eligibility requirements to be closely associated with the clearly delineated community invoked and pay annual membership). As an additional point, the significance and applicability of “formal boundaries” was rejected. It is known that formal boundaries are in place to facilitate a delineated process in which rights holders are compensated and to eliminate piracy and copyright infringement e.g. Objector member iTunes formally requires hundreds of millions of music fans to create formal Apple accounts and abide to strict terms of service to consume music and to ensure that royalties are paid using clearly delineated, organized systems that identify rights-holders corresponding to each song sold or streamed (Annex F, G, I). In fact, the Expert denies such delineated structured systems such as the ISMN, ISRC, ISWC, ISNO and other systems used to classify

[29] U.S Department of Labor, http://www.bls.gov/oes/current/oes272042.htm

[30] http://www.billboard.com/biz/articles/news/digital-and-mobile/1556590/ifpi-2013-recording-industry-in-numbers-global-revenue

[31] https://community.icann.org/display/newgtldrg/community+objection+grounds

[32] http://newgtlds.icann.org/en/applicants/agb/string-contention-procedures-04jun12-en.pdf, Module 4-11

[33] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfJAXl5xkyLm.pdf

[34] http://www.onlineaccountability.net/pdf/2012_Mar06_ICANN_EnhancedSafeguards.PDF

[35] http://www.musicunited.org/1_whocares.aspx

[36] musicFIRST Coalition, with founding members A2IM, RIAA, and Recording Academy represents musicians, recording artists, managers, music businesses, performance right advocates. http://musicfirstcoalition.org/coalition

[37] http://www.copyrightalliance.org/members

[38] U.S Government International Trade Commission, http://www.usitc.gov/publications/332/pub4393.pdf, 3-9 and C-3, http://www.usitc.gov/search-ui/search/C.view=default/results?s=&sa=0&hf=20&q=A2IM, May 2013

music and compensate rights holders (EXP/474/ICANN/91, ¶29, P.9) claiming that "this cloud of words does not convey anything which can be fairly be described as a clearly delineated community" (EXP/474/ICANN/91, ¶30, P.9). If such a clearly delineated community invoked does not exist then the Expert failed to explain how the community's invoked rights holders get paid from royalties, such as statutory or performance royalties determined by governments and enforced by law. Without formal boundaries and Safeguards, the strictly delineated compensation system that exists would be compromised in favor of piracy and abuse which already is rampant.

The Expert contends that in regard to Objections, "if the fear was really well founded the entire world record industry would be up in arms… The absence of a universal clamour makes it clear to me that the record industry as a whole does not fear material detriment." (EXP/477/ICANN/94, ¶44, Pg. 12). Again, the Expert ignored the overwhelming evidence presented by the Objector with respect to the invoked community's fears of piracy, anti-competitive issues and abuse for music-themed gTLDs. Globally-recognized, highly-credible associations strongly associated with strings (and others) voiced serious concerns of the high likelihood of material harm without Safeguards. These included public comments[39] by the Coalition of Online Accountability (included A2IM),[40] the Copyright Alliance (included A2IM),[41] Austrian Music Industry Association,[42] International Publishers Association,[43] BREIN Copyright Industry Groups,[44] as well as ICANN's Business Constituency[45] and Intellectual Property Constituency[46] and many others. **These substantial public comments by A2IM and others mirrored the concerns made by the banking industry whose Objection was upheld against Radix (whose .bank application was nearly identical to their .music objected-to application)** citing their lack experience and lack of existing relationships in a highly complex regulatory environment:

> [H]ighly likely to result in inadvertent non-compliance with bank regulatory measures, in delays in obtaining regulatory consents, in difficulties resolving overlapping requirements imposed by a multiplicity of regulators and policymakers, and in significant concerns on the part of regulatory authorities over the possibility of fraud, consumer abuse, tax evasion and money laundering, other financial crimes and improper avoidance of regulatory measures by means of the Internet. (DotSecure Determination, ¶163, 32)

There the Expert that upheld the .bank Objection noted that concerns were highlighted by bank regulatory authorities in their comments to ICANN – just as in the case of the community invoked expressing

[39] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/
[40] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfykweBGd8BS.pdf
[41] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfZAxxvKEQJa.pdf
[42] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfqbAFJIXCE4.pdf
[43] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/binYYWrklmmsT.bin
[44] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/msg00093.html
[45] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfmAs6qFAMCk.pdf
[46] http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfzg5FzsaA92.pdf

identical concerns for music-themed sensitive strings (emphasis added). Similarly, an Objection was upheld against Famous Four's .sport (whose .sport application was nearly identical to their .music objected-to application). Even though the Expert asserted that some detriments alleged by Objector SportAccord were "purely hypothetical", the Expert concluded that there was a "strong likelihood of material detriment to the rights or legitimate interests of the Sport Community if the application ... is allowed to proceed" and that Objector "proved several links between potential detriments" that the community may suffer and the operation of the .SPORTS string (dot Sport Determination, Pg. 24, ¶163 and Pg. 23, ¶¶157-58).

Additionally, other Experts upheld Objections to "open" applicants relating to sensitive strings were upheld (.insurance, .charity, .med, .sport, .sports and bank) against all the same objected-to Applicants for music-themed strings. It is reasonable to conclude that if Objectors met standing (through application of the appropriate standard) that material harm pertaining "open" music-themed sensitive strings would also be upheld in the instant music related cases. However, because standing was not determined, Expert did not assess "material harm" and concerns of community invoked were not heard.

The Expert also introduces a new test to require an Objector to evaluate and compare other gTLD Applications and contention "rivalries" which are not part of an Objection dispute since the Community Objection process is not a "beauty contest" to compare Applications. The Expert also made false speculations that the purpose of the Objection is to eliminate a rival applicant:

> "DotMusic" appears to be the general name of this rival. Its moving spirit is Mr Constantinos Roussos, named as the Objector's representative in this case. Such support would include eliminating a rival applicant (EXP/474/ICANN/91, ¶19, Pg. 6)

The Objector's representatives (or any rival Applications) are irrelevant to each objected-to case, but the Expert created a new test seeming to require the Objector to compare or comment on other Applications to justify the high likelihood material harm indicating that:

> The Objector cannot be heard to say that any music gTLD will cause material harm for it does not object to Mr Roussos' application. Its position in logic must be that his application would cause no detriment but this would. That it has not tried to do (EXP/462/ICANN/79, ¶42, 11)

In fact, the Objectors clearly articulated the material detriment in each corresponding case relating to Safeguards. The Expert failed to grasp the dangers of "open" strings and falsely concludes that "no doubt ICANN will have remedies" if there are violations (EXP/462/ICANN/79, ¶44, Pg. 12) when in fact ICANN is not a "copyright" enforcer and none of ICANN's policies in the new gTLD Program directly tackle copyright, the DMCA, EDEC and piracy[47] which negatively affects clearly delineated community invoked.

More worrisome is the Expert calling the Google Transparency Reports (e.g 80 million copyright infringement URL removals from just 2 organizations the RIAA and BPI last year[48]) on mass copyright infringement[49] and studies conducted by McAfee, Namesentry, Verisign and Symantec (which overwhelmingly prove that open gTLDs are significantly riskier than restricted gTLDs) "irrelevant":

> I fail to see what these general reports have to do with the proposed string. They are not concerned with it – their concern is much more general – about open or closed strings… I therefore hold that these reports are irrelevant (EXP/460/ICANN/77, ¶26 and ¶27, Pg. 10).

The evidence is overwhelming pertaining to the likelihood of material harm for sensitive strings under an "open" gTLD system, especially in a regulated market which involves copyright. Other examples proving likelihood of harm caused by "open" systems without Safeguards is Android's open system. Google Android's open app ecosystem "does not have a strict process to block pirated or malicious applications[50] – analogous to objected-to Applicants "open" policies, making it highly vulnerable to abuse."[51] Google's open platform stats reveal that: (i) 72% of all its apps access at least one high-risk permission,[52] (ii) Malware increased by 580% between 2011 to 2012 with over 175,000,000 downloads deemed "High Risk,"[53] (iii) Kaspersky Lab: 99% of mobile malicious programs target Google Play's open platform.[54] In antithesis, Apple App Store has a stricter and more restrictive approval process which is safer and less vulnerable to abuse.[55]

Also, in many instances the Expert relied on false or misleading information that was clearly not verify for accuracy. For example, in conclusions, the Expert determined that A2IM – the Objector that Constantinos Roussos represented in Objections – is a supporter of DotMusic, which is untrue. The Expert's final conclusion Points (¶37, ¶38 and ¶39) pertaining to "detriment" were also based on errors and false facts that were not verified:

> "…the Objection itself is not to .band in principle (rather, A2IM is supporting Mr Roussos's application

[47] Music Coalition letter to ICANN, http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/msg00092 html (http://forum.icann.org/lists/comments-gac-safeguard-advice-23apr13/pdfJAXl5xkyLm.pdf

[48] https://www.google.com/transparencyreport/removals/copyright/owners/?r=last-year

[49] http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=clear-facts-&blog_type=&news_month_filter=5&news_year_filter=2012

[50] www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

[51] http://www.pcmag.com/article2/0,2817,2396558,00.asp

[52] https://www.bit9.com/download/reports/Pausing-Google-Play-October2012.pdf

[53] http://blog.trustgo.com/image/2012/10/trustgo_halloween_spotlight.pdf

[54] http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012#1

[55] http://www.wired.com/business/2012/12/ios-vs-android/

> for .band)"(EXP/459/ICANN/76, ¶38, P.10) …At the very least, since it supports Mr Roussos' application for .band, the Objector should have demonstrated how that Application would not cause detriment but this one would" (emphasis added)." (EXP/459/ICANN/76, ¶39, P.10)

These Expert statements prove the Expert lacked appropriate training for this particular process. Such material error include the fact that Roussos did not apply for .band. Moreover this point would not be relevant for the "material detriment" test. It can be verified[56] that Whatbox (Red Triangle) and Donuts (Auburn Hollow) were the only Applicants for .band. Furthermore, A2IM did not support any .band Application and did not support an Application by Roussos. Determinations decided on the basis of false information or/and incorrect AGB procedures and tests hold absolutely no ground to be upheld and must be dismissed by the BGC. The unintended consequences of allowing false information to determine cases puts in question ICANN's own credibility and Bylaws.

As to Point 3: lack of an appeal process for Community Objections thereby denying parties procedures to protect their fundamental rights. The failure of the Board to address a chorus of voices that called for an appeal mechanism to allow appropriate review of cases has prejudiced Objector's ability to protect their members' fundamental and legitimate rights. ICANN's lack of action forced the parties to: a) bear significant expense; b) detrimentally rely on ICANNs stated policies and procedures for Community Objections; c) led to a breach of process; d) has resulted in process in which Applicants will be able to materially change their positions (e.g. from an exclusive access registry to an open registry or adding PICs not in their current Applications); and e) resulted in the selection and appointment of an expert that was not prepared to address the unique issues presented.

As a result of the Decisions, the Affected Parties suffered direct financial harm in order to prepare and file the Objections. The Affected Parties will also suffer financial harm, and the Objectors' community invoked will be negatively affected should the objected-Applicants be ultimately be awarded these music-themed gTLDs.

### 7. Describe how others may be adversely affected by the action or inaction, if you believe that this is a concern.

Other groups adversely affected by the inaction are community applicants who have serious concerns about the unintended consequences and precedents created in the new gTLD Program in relation to material changes[57] which are inconsistent to the AGB. Such Material Changes by Applicants (through PICs and other Safeguards) have no consequences or accountability mechanisms to protect community

[56] https://gtldresult.icann.org/application-result/applicationstatus/viewstatus

[57] http://newgtlds.icann.org/en/applicants/customer-service/change-requests

applicants in a contention set. In context, Community Applications already abide to the Registry Dispute Resolution Procedure (RRDRP) built-in accountability mechanism.[58] Community Applicants also have appropriate restrictions, including policies relating to Eligibility, Name Selection, Content/Use, and Enforcement to safeguard their communities.

Changes of position occurring during Community Objection proceedings not found in current Applications indicates procedural flaws of Community Objection process and also vindicate Community Objectors' positions. ICANN has even took this issue a step further by revising the new gTLD Registry Agreement during Objection proceedings with language vindicating Objectors views. According to the AGB, any information that is deemed "false or misleading may result in denial of the application."

Such Material Changes significantly change an Applicant's business model and other critical components in their Application, such as financial statements and their Letter of Credit. Under the ICANN AGB rules such material "changes" will likely "involve additional fees or evaluation in a subsequent application round." As such, the existing new gTLD process has lost meaning since any Applicant is now allowed to "shift" their position without accountability of any sort or ICANN action to prevent such violations. As such, many Objectors were materially harmed by Determinations since Experts lacked fundamental knowledge of community functions. Also Determinations based on false facts and relying on contradictory AGB standards for standing might harm Community Applicants in CPE.

## 8. Detail of Board or Staff Action – Required Information

On June 19th 2013, a letter was sent to ICANN and the Board which raised serious concerns that "the ICC has not identified expert Panelists that have expertise in music - the relevant subject matter of interest for the communities." On June 24th, 2013 ICANN responded stating that "for the matter of the expertise of the panel members…Section 3.4.4 of the Applicant Guidebook" states:

> 3.4.4 Selection of Expert Panels - A panel will consist of appropriately qualified experts appointed to each proceeding by the designated DRSP. Experts must be independent of the parties to a dispute resolution proceeding. Each DRSP will follow its adopted procedures for requiring such independence; including procedures for challenging and replacing an expert for lack of independence

ICANN further stated in their response that "ICANN has confidence that the ICC has followed the requirements as expressed by the AGB and has appointed experienced jurists with appropriate qualifications in mediation/arbitration to preside over objection proceedings."

[58] http://www.icann.org/en/news/public-comment/rrdrp-15feb10-en htm

However, ICANN's response that the "appropriate qualifications" of an expert is in "mediation/arbitration" is not mentioned in the AGB. The definition of "expert" is "a person who has a comprehensive and authoritative knowledge of or skill in a particular area.[59]" Objectors reasonably relied on the fact that experts would be "appropriately qualified experts" pertaining to the Applications determined and have "comprehensive and authoritative knowledge" in that "particular area."

ICANN solicited Responses from Applicants for the strings identified by GAC Advice whether they planned to operate strings as exclusive access registries (defined as a registry restricted to a single person or entity and/or that person's or entity's Affiliates" (Section 2.9c of the Registry Agreement).

.MUSIC (DotMusic) sent written correspondence to ICANN, the ICC and Expert on Material Changes and process issues relating to Community Objections that ultimately created harm to Objectors, 3rd-parties and Community Applicants (Annex J). The Expert – despite correspondence – failed to investigate the material detriment issues of exclusive access that were presented in cases and did not give standing in any Determination (e.g EXP/474/ICANN/91). Pertinent "material detriment" issues were never heard. ICANN did not act in accordance to its ByLaws and has put in motion new processes to "fix" objected-to Applicants' Safeguards without any accountability at the expense of Objectors and 3rd-parties. ICANN also did not invite .music LLC to submit a change request (as it did with Amazon) despite its current Application's exclusive access language (e.g having a "sole registry" and only allowing Accredited Associations formed before 2007 ("Affiliates") to offer .music to members (i.e. excluding members of legitimate organizations formed after 2007 or non-"Accredited" Affiliates (Annex J).

Both the ICANN Board and the NGPC responded to the GAC Advice and called for public comment and input regarding "closed generic" Category 2 Applications and took action to materially change how such gTLDs are to be operated and allowed Applicants to intentionally materially change their Applications, in some cases from an exclusive access registry to a non-exclusive registry. During the proceedings ICANN put in motion a process which would ultimately allow Material Changes to Applications in the form of new binding contractual amendments. During this process ICANN failed to respond to Objector's stated concerns about the effect of GAC Advice on the proceedings and failed to advise the ICC and Expert to consistently align itself with both GAC Advice and NGPC Resolutions.

**The Affected Parties believe that there was inaction by ICANN:**

1) in failing to adequately train, advise, and instruct the ICC, thus allowing the ICC to appoint an expert who was unqualified to address the specific issues related to community invoked, its composition, strict delineation and host of intellectual property DNS issues e.g piracy;

[59] Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/expert

2) by refusing to present to ICC and Expert, GAC-related issues and new NGPC Resolutions: Responses to GAC Advice, PICs, Board Resolutions, Changes in Applicant positions through the GAC Advice Category 2: Exclusive Access Response Form for Applicants, and revisions to Registry Agreement that addressed GAC Advice allowed the Objection to proceed without consideration of the effect and importance of these exceptional developments that occurred after the Objections were filed;

3) by allowing a process to facilitate modifications and material changes to Applications as PICs, or, in response to GAC Advise on Category Exclusive Access Applications, permitted Applicant's to fundamentally change positions during proceedings without ramifications to detriment of Objector;

4) in creating a process by which exceptional modifications and material changes to Applications in response to GAC Advise can be facilitated. Failing to address the effect of such actions to ongoing Objections violated Article 4 of the Articles of Incorporation and Article 1, Section 2, 7, 8, and 9 of the ICANN Bylaws resulting in a breach of process and calls into question the legitimacy of the Program; and

5) by failing to offer an appropriate appeal mechanism to address clear procedural issues and AGB violations pertaining to Objections especially in cases of unqualified panels using factually incorrect and inconsistent statements and applying contradictory standards.

6) by harming applicants in a contention set as well as Community and Legal Rights Objectors against objected-to .music Applicants who relied on the AGB's language.

7) in failing to ensure there were no conflicts of interest and bias in panels relating to the new gTLD Objection process as whole. This compromises the credibility of the new gTLD program and sheds light on how Objections were mishandled by ICANN without any accountability on the selection of panels even if there was a clear conflict of interest. Whether Expert signed a statement of independence and disclosed it to the ICC does not prove there was no conflict of interest or inherent bias from the Expert.

### 9. What are you asking ICANN to do now?

1) Reimburse or order the ICC to reimburse the Objector for all of its expenses, including but not limited to attorney fees, administrative expenses and Expert fees associated with cases: ICC EXP/462/ICANN/79 (c. EXP/463/ICANN/80, EXP/467/ICANN/84, EXP/470/ICANN/87 EXP/477/ICANN/94), ICC EXP/474/ICANN/91, ICC EXP/459/ICANN/76, ICC EXP/460/ICANN/77;

2) Allow new Community Objections be filed for these cases with appropriate music Expert;

3) Determine that objected-to .music LLC's GAC Responses (that they do not intend to be exclusive access registry) be deemed material and inconsistent with their position in Community Objection Responses and policies in their current Application and initiate a change request for Applicant 1-959-

51046 to reflect such material changes pertaining to removing exclusive access language (Annex J) since it violates the AGB (1.2.7) stating that at any time during the evaluation process information previously submitted becomes untrue or inaccurate, the applicant must notify ICANN of such changes. As evidenced in Annex J, information provided was misleading. According to ICANN "Failure to notify ICANN of any change in circumstances that would render any information provided in the application false or misleading may result in denial of the application."[60]

4) Allow for a Reconsideration of the Decisions by an appropriate and qualified expert and with instruction regarding the GAC Advice and changes made by Applicants.

**10. Please state specifically grounds under which you have the standing and the right to assert this Request for Reconsideration, and the grounds or justifications that support your request.**

DotMusic Limited (.MUSIC) is community Applicant for .music and Objector Representative. All Applicants and Objector(s)/Related-Objector Entities are entitled to a fair and appropriate evaluation of procedures. .MUSIC (as a community applicant) could be adversely affected in CPE by Determinations (which relied on contradictory standards and false information). If CPE fails, .MUSIC will be subject to expensive auctions which - as agreed upon by the EU[61] - were designed to favor deep pocketed Applicants – such as Amazon and Google.

Breach of Fundamental Fairness: Basic principles of due process to proceeding were violated and lacked accountability by ICANN, ICC and Expert despite the excessive costs and resources attributed to filing.

Failure to Consider Evidence: Expert failed to consider relevant evidence relating to: (i) Material Changes and Safeguards; (ii) Standing of Objector as a clearly, delineated community invoked expressing opposition; (iii) Substantial size/ global breadth of Objectors/Related Entities and strong association with music-themed strings;

Violation of ICANN Articles of Incorporation: Article 4 calls ICANN to operate for the benefit of Internet community as a whole, carrying out activities in conformity with relevant principles of international law and applicable international conventions and local law, and to the extent appropriate and consistent with its Articles and Bylaws, through open and transparent processes that enable *competition and open entry in Internet related markets.* ICANN should have properly communicated and delegated functions to the ICC but failed to do so in violation of ByLaws Art. 1, Section 2, 3: *To the extent feasible*

[60] http://newgtlds.icann.org/en/applicants/customer-service/change-requests
[61] http://forum.icann.org/lists/comments-new-gtld-auction-rules-16dec13/msg00016.html

*and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties*. (ByLaws Art. 1, Section 2, 7 *Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most affected can assist in the policy development process*; ByLaws Art. 1, Section 2, 8 *Making decisions by applying documented policies neutrally and objectively, with integrity and fairness*.

**11. Are you bringing this Reconsideration Request on behalf of multiple persons or entities?** Yes

**11a. If yes, Is the causal connection between the circumstances of the Reconsideration Request and the harm the same for all of the complaining parties?**

The clearly delineated community invoked (i) has a shared, common interest - the <u>legal</u> distribution and promotion of music, (ii) is dependent on DNS (where rampant piracy occurs – Annex F, I) for core activities, and (iii) Determinations of such significance pertaining to enhanced safeguards, competition and exclusive access can create material detriment to legitimate interests of significant portion of the community invoked. Failure of Expert to understand such issues exhibits why these cases require a music expert.

**Do you have any documents you want to provide to ICANN?** Yes, see Annexes A-L

**Terms and Conditions for Submission of Reconsideration Requests:**

The Board Governance Committee has the ability to consolidate the consideration of Reconsideration Requests if the issues stated within are sufficiently similar. The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious. Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing. The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC. The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.

___________________________________

Constantinos Roussos - .MUSIC (DotMusic)　　　　　Date: March 4th, 2014

# Appendix D

## Original Amazon Applications for .MUSIC, .SONG and .TUNES

# New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

## String: MUSIC

## Originally Posted: 13 June 2012

## Application ID: 1-1316-18029

# Applicant Information

## 1. Full legal name

Amazon EU S.à r.l.

## 2. Address of the principal place of business

Contact Information Redacted

## 3. Phone number

Contact Informat on Redacted

## 4. Fax number

Contact Information Redacted

## 5. If applicable, website or URL

http://www.amazon.com/

## Primary Contact

### 6(a). Name

Ms. Lorna Jean Gradden

### 6(b). Title

Operations Director

### 6(c). Address

### 6(d). Phone Number

Contact nformation Redacted

### 6(e). Fax Number

Contact nformation Redacted

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Ms. Dana Brown Northcott

### 7(b). Title

Associate General Counsel, IP

### 7(c). Address

### 7(d). Phone Number

Contact  nformation Redacted

### 7(e). Fax Number

Contact  nformation Redacted

### 7(f). Email Address

Contact Information Redacted

## Proof of Legal Establishment

### 8(a). Legal form of the Applicant

Corporation (Société à responsabilité limitée)

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

Luxembourg

### 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.

Amazon Europe Holding Technologies S.C.S. (AEHT) owns 100% of Amazon EU S.à r.l.  AEHT is held by one unlimited partner, Amazon Europe Holdings, Inc. and two limited partners, Amazon.com, Inc. and Amazon.com Int’l Sales, Inc.

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

Amazon EU S.à r.l. is not a joint venture.

## Applicant Background

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Amazon Europe Holding Technologies S.C.S. | 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.

MUSIC

## 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.

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

## 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.

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the .MUSIC registry is:
To provide a unique and dedicated platform for Amazon while simultaneously protecting the integrity of its brand and reputation.
A .MUSIC registry will:

- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

## 18(b). How do you expect that your proposed gTLD will benefit registrants, Internet

## users, and others?

The .MUSIC registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?
Amazon intends for its new .MUSIC gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The .MUSIC registry will be run in line with current industry standards of good registry practice.
What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?
Amazon values the opportunity to be one of the first companies to own a gTLD. A .MUSIC registry will:
- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

What goals does your proposed gTLD have in terms of user experience?
Amazon intends for its new .MUSIC gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.
Provide a complete description of the applicant’s intended registration policies in support of the goals above
Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a .MUSIC domain name, and (iii) the dispute resolution policies for the .MUSIC gTLD. Amazon will continually update the Domain Management Policy as needed to reflect Amazon’s business goals and, where appropriate, ICANN consensus policies.
Registration of a domain name in the .MUSIC registry will be undertaken in four steps: (i) Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration. All domains in the .MUSIC registry will remain the property of Amazon.
For example, on the rules of eligibility, each applied for character string must conform to the .MUSIC rules of eligibility. Each .MUSIC name must:
- be at least 3 characters and no more than 63 characters long
- not contain a hyphen on the 3rd and 4th position (tagged domains)
- contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
- start and end with an alphanumeric character, not a hyphen
- not match any character strings reserved by ICANN
- not match any protected country names or geographical terms

Additionally:
- Internationalized domain names (IDN) may be supported in the .MUSIC registry at the second level.
- The .MUSIC registry will respect third party intellectual property rights.
- .MUSIC domains may not be delegated or assigned to third party organizations, institutions, or individuals.
- All .MUSIC domains will carry accurate and up-to-date registration records.

Amazon’s Intellectual Property group reserves the right to revoke a license to use a .MUSIC domain name, at any time, if any use of a .MUSIC domain name violates the Domain Management Policy.
Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?
Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.
Describe whether and in what ways outreach and communications will help to achieve your projected benefits?
There is no foreseeable reason for Amazon to undertake public outreach or mass communication about its new gTLD registry because domains will be provisioned in line with Amazon’s business goals.

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

Amazon intends to initially provision a relatively small number of domains in the .MUSIC registry to support the business goals of Amazon. These initiatives should not impose social costs of any type on consumers.
How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?
Applications from Amazon and its subsidiaries for domains in the .MUSIC registry will be considered by Amazon’s Intellectual Property group and allocated in line with Amazon’s business goals. The .MUSIC registry will not be promoted by hundreds of registrars simultaneously, so there will not be multiple-applications for a particular domain.
Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).

Domains in the .MUSIC registry will be provisioned to support the business goals of Amazon. Accordingly, “cost benefits” may be explored depending on the business goals of Amazon.  Amazon shares the goals of enhancing customer trust and choice.
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 10 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?
The Domain Management Policy will include the costs and benefits of Amazon’s unique and dedicated platform for stable and secure online communication and interaction.

# 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.

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as “Amazon”), is committed to managing the .MUSIC registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement.  In the management of domain names in the .MUSIC registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration those country and territory names contained in the following lists:

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; and
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
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.

The process for reserving these names, and hence blocking them from registration, will be agreed to with our technical service provider Neustar.

Because the .MUSIC registry will be a single entity registry and for purposes which serve Amazon’s strategic business aims, the reserved names cannot be offered to Governments or other official bodies for their own use as this would conflict with the mission and purpose of the gTLD.  However, for the same reason, they will not be offered to third parties.

The .MUSIC registry only provides for the registration of names at the second level.  No third level domains will be delegated at the registry level.  It is consistent with GAC advice that Amazon may choose to create sub domains using country names or abbreviations at the third level.  For example, Amazon may register information.music and its internal users may create sub domains such as us.information.music or uk.information.music.

Amazon may also use a folder structure to represent country names in its URLs, while the block exists at the second level.  For example, information.music⁄germany or information.music⁄uk.

We imagine that over time, there will be demand from brand gTLDs leading to the development of a standardized process for requesting GAC review and ICANN approval for the release of country and territory names for registration by the Registry Operator when the registry is a single entity registry.  When such a process is in place, Amazon expects to apply for the release of country and territory names within .MUSIC.

# Registry Services

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .MUSIC registry. In making this decision, Amazon EU S.à r.l. 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 .MUSIC 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. Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .MUSIC registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .MUSIC.

- 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 .MUSIC 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

Amazon EU S.à r.l. 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 .MUSIC. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy 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

Amazon EU S.à r.l. 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 .MUSIC 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

Amazon EU S.à r.l. 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

Amazon EU S.à r.l. will not be offering services that are unique to .MUSIC.

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.

# Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

24.1 Introduction

Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .MUSIC Registry. Amazon EU S.à r.l. 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 .MUSIC 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, Amazon EU S.à r.l. 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 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 Amazon EU S.à r.l., 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 initiates 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 components 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 .MUSIC 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 .MUSIC.

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 .MUSIC 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 .MUSIC 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 .MUSIC 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 .MUSIC registry.

## 25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

Amazon EU S.à r.l.'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 Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .MUSIC 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.

25.4 Proprietary EPP Extensions

The .MUSIC 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 .MUSIC 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 .MUSIC registry is attached in the document titled “EPP Schema.”

25.5 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 .MUSIC registry.

## 26. Whois

26.1 Introduction
Amazon EU S.à r.l. 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. Amazon EU S.à r.l.'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 .MUSIC's 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, .MUSIC's 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 (www.whois.MUSIC). 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 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.

Potential Forms of Abuse

As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois 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 .MUSIC 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 .MUSIC registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .MUSIC registry.

# 27. Registration Life Cycle

27.1 Registration Life Cycle
Introduction
.MUSIC 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 .MUSIC.
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 .MUSIC registry per the defined .MUSIC 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 .MUSIC 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 .MUSIC 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 .MUSIC 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 .MUSIC 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 general establishes the maximum term of a domain name to be 10 years, and Neustar recommends 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:

4. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
5. 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
6. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar’s message queue
7. 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

8. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer

9. 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 with Amazon EU S.à r.l. 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 .MUSIC 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 .MUSIC registry.

## 28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the .MUSIC registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar's extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed .MUSIC space.

.MUSIC will be a single entity registry, with all domains registered to Amazon for use in pursuit of Amazon's business goals. There will be no re-sellers in .MUSIC and there will be no market in .MUSIC domains. Amazon will strictly control the use of .MUSIC domains. Opportunities for abusive and malicious domain activity in .MUSIC are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

Illegal or fraudulent actions

Spam

Phishing

Pharming

Distribution of malware

Fast flux hosting

Botnets

Malicious hacking
Distribution of child pornography
Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.'s registry services provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a "domain takedown" policy. Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.

Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry. Amazon EU S.à r.l., via Neustar, 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.

Abuse Point of Contact

As required by the Registry Agreement, Amazon EU S.à r.l. 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 conduct. Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in .MUSIC. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made. In addition, the registry services provider for .MUSIC, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in .MUSIC; (ii) reserves Amazon EU S.à r.l.'s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its .MUSIC Acceptable User Policy into its Registry-Registrar Agreement.

Under the .MUSIC Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name "on hold" rendering the domain name non-resolvable, transfer the domain name to another registrar and/or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.'s intention that all .MUSIC domain names will be registered and used by it and its Affiliates and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register .MUSIC domain names. Accordingly, the potential for abusive registrations and malicious conduct in the .MUSIC registry is expected to be limited. In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities. Below is initial Acceptable Use Policy for the .MUSIC registry.

.MUSIC Acceptable Use Policy

This Acceptable Use Policy gives the .MUSIC registry the ability to quickly lock, cancel, transfer or take ownership of any .MUSIC 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 .MUSIC 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 .MUSIC 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 .MUSIC registry or its partners. In all cases, the .MUSIC registry or its designees will alert .MUSIC 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: the attempt to acquire personally identifiable information by masquerading as a website other than .MUSIC's own.

Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.

Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.

Fast Flux 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 address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.

Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.

Malicious 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.

Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The .MUSIC registry reserves the right, in 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 .MUSIC 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, in 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 .MUSIC 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 .MUSIC registry or any Registrar in connection with a domain name registration. The .MUSIC registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The .MUSIC registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the .MUSIC 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 registry’s ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the .MUSIC registry will place the domain on “ServerHold”. (It is unlikely the registrar will not timely act because Amazon EU S.à r.l. intends to use a single, gateway registrar with which it has a contract reflecting these policies). ServerHold removes the domain name from the .MUSIC zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the .MUSIC registry. The .MUSIC registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The 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 Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the .MUSIC Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .MUSIC Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, .MUSIC’s registry services provider, has developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar/registrant relationship.

Amazon EU S.à r.l.’s restrictions on registration eligibility make it unlikely that any .MUSIC domains will be taken down. The .MUSIC registry rules are anticipated to exclude third parties beyond Amazon EU S.à r.l. and its Affiliates. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register .MUSIC domain names.

Neustar’s active prevention policies stem from the notion that registrants in .MUSIC have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by “typical” notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below, though it is important to note that .MUSIC will be managed as a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon’s subsidiaries. Therefore, the potential for abusive registrations and other activities that have a negative impact on Internet users is minimal. In the unlikely event that such abuse should occur, Amazon with its registry operator, Neustar, will implement the following policies and processes to manage such activities.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the .MUSIC registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar’s internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar’s operations, legal, support, engineering, and security teams for immediate response (“CERT Team”). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual’s own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar’s internal or external network elements are harmed in any fashion.

Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone.

The .MUSIC Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

ServerHold removes the domain name from the .MUSIC zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event with a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon’s subsidiaries, that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the .MUSIC registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.

Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact Amazon EU S.à r.l.’s registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident. As .MUSIC is a Single Entity Registry using a single registrar whose work will be strictly controlled through a Service Level Agreement that includes the implementation of measures to prevent abusive registrations, the risk of evidence of abuse being compromised is minimized. Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.

Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries’ TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its .MUSIC registry. Amazon EU S.à r.l. and⁄or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such 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 Amazon EU S.à r.l. and⁄or Neustar for rapid resolution of the request.

If the request involves any of the activities that can be validated by the registry and⁄or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .MUSIC registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

28.3 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 often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the .MUSIC registry has written evidence of actual abuse of orphaned glue, the .MUSIC registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.
In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The .MUSIC registry will implement several measures to promote Whois accuracy.
Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.’s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The Amazon EU S.à r.l.’s registrar will also be charged with regularly checking Whois accuracy.
Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the Amazon EU S.à r.l. registrar who will have a contractual duty to comply with Amazon EU S.à r.l.’s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.’s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.’s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN’s Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN’s Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Only Amazon EU S.à r.l. and its Affiliates will be permitted to register and use Amazon EU S.à r.l. domain names. Accordingly, the duties of the Amazon EU S.à r.l. registrar will be very limited and closely defined. Regardless, Amazon EU S.à r.l.’s Registry-Registrar Agreement will require Amazon EU S.à r.l.’s registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the .MUSIC registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar 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:
Customer Support – 12 employees
Policy/Legal – Two employees
The resources are more than adequate to support the abuse mitigation procedures of the .MUSIC registry.
Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.
The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes experts in Amazon EU S.à r.l.’s registrar where one legal manager and four operational experts will be available to support Amazon EU S.à r.l.

Please note that in the above answer the terms “We”, “Our” and “Amazon” may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

## 29. Rights Protection Mechanisms

29.1 Introduction
Amazon is applying for .MUSIC to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.
29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon
We will closely manage this TLD by registering domains through a single registrar. Although Amazon and its subsidiaries will be the only eligible registrants, we will nonetheless require our registrar to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will remain the property of Amazon and will be provisioned to support the business goals of Amazon. Because all domains will be registered and maintained by Amazon (for use that complements our strategic business goals), we can ensure that all domains in our registries will carry accurate and up-to-date registration records.
We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.
29.2 Core measures to prevent abusive registrations
To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:

- A 30 day Sunrise process
- A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered only to Amazon or its subsidiaries through a single registrar who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.
In the very unlikely circumstances that a domain is registered and used in an improper way, we acknowledge that we will be the respondent in related proceedings and we undertake to co-operate fully with ICANN and other appropriate agencies to resolve any concerns.
29.2.1 Sunrise Eligibility
Our Sunrise Eligibility Requirements will clearly state that eligible applicants must be members of the Amazon group of companies and its subsidiaries. Furthermore, all domain names must be used to support the business goals of Amazon. Nonetheless, notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.
29.2.2 Sunrise Window
As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize “all word marks: (i) nationally or regionally 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; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008”.

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will have a one year term of registration. Any domain names registered will be managed by our registrar.
29.2.3 Sunrise Dispute Resolution Policy
We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will apply to all our registries and will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):
(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.

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by our registrar. Our registrar will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service

Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honour and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by our registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)

Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.

Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

The Implementation Team will create a formal Registry Launch plan by 1 October 2012. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will be built by 1 December 2012 or within 30 days of pre-validation testing beginning, whichever is the sooner. It will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrar (the RAA) will require that the registrar uses the TMCH, adheres to the Terms & Conditions of the TMCH and will prohibit the registrar from filing domains in our registries on its own behalf or utilizing any data from the TMCH except in the provision of its duties as our registrar.

When processing TMCS claims, our registrar will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.

We will also require our registrar to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.
- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.
- The Post Delegation Dispute Resolution Procedure (PDDRP).
- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries. As domains in our registry will be registered not to third parties but only to Amazon or its subsidiaries through a single registrar which will be required through contract to ensure that the rules covering eligibility and use of a domain are adhered to, we believe that abusive registrations by third parties should be completely prevented.

Abusive behaviour by representatives of Amazon or our subsidiaries will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrar.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints against us, as the registrant, are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith. In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

Amazon or its subsidiaries will be the respondent in all UDRP complaints because we will be the only eligible registrants. Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no rights or legitimate interests” in a domain in our registry so the possibility of good faith UDRP complaints should be minimized. In the unlikely circumstances that a complaint is made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.

We will be applying for an exemption to Clause 1b of the Registry Operators Code of Conduct. This means that we will not be allowed to transfer domains to third parties as the only registrant will be Amazon or our subsidiaries. Therefore if a complaint against us is filed, the only possible remedy will be the cancellation of the domain instead of the transfer to the complainant.

Should a successful complaint be made we will therefore place the cancelled domain that is the subject of the complaint on a list that prevents it from being registered again.

29.3.2 The URS

The URS is intended to be a lighter, quicker complement to the UDRP. Like the UDRP, it is intended for clear-cut cases of trademark abuse. Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences. Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year. Either party may file a de novo appeal within 14 days of a decision. There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

As with the description of our UDRP process above, Amazon or its subsidiaries will be the respondent in all URS complaints because we will be the only eligible registrants. Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no legitimate right or interest to the domain name” and “that the domain name was registered and is being used in bad faith.” Notwithstanding this, should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator. Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.

We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

Being the only eligible registrant, we will not make changes to a domain in Locked Status or alter a registration record associated with a URS complaint as required in the Applicant Guidebook.

29.3.3 The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse. In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms. The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarising the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant’s mark or (ii) impairs the distinctive character or the reputation of the complainant's mark, or(iii) creates a likelihood of confusion with the complainant's mark.”

Whilst we will co-operate with any complaints made under the PDDRP and we will abide by any determinations, we think it is highly improbable that any PDDRP complaints will succeed because the grounds set out above cannot be satisfied as domains in the registry will not be for sale and cannot be transferred to third parties.

29.3.4 Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois. A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars). Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on our registrar to ensure that all registrations are filed with accurate Whois details and we will undertake reviews of Whois accuracy every three months to ensure that the integrity of data under our control is maintained.

Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

29.3.5 Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring our registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.
- Confirming the implementation of the lock to the relevant URS provider, and ensure our registrar confirms the implementation of the lock to the relevant UDRP provider.
- Ensuring that our registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours
- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for a registry where the only registrant is Amazon or its subsidiaries. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require our registrar to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see: http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.

An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.

The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

29.4.3 Registrar Accreditation

Amazon will audit the performance of our registrar every six months and re-validate our Registry-Registrar Agreements annually. Our audits will include site visits to ensure the security of data etc.

29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed by our registrar to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

29.4.6  Click Wrapping our Terms & Conditions

Although only Amazon and its subsidiaries can register domain names in our registry, we will bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

29.4.7  Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website.  This will include relevant statistics and it will outline all cases and how they were resolved.

29.4.8  Contacts with WIPO and other DRS providers

Amazon will invite representatives of WIPO and other DRS providers to review our RPM and to make suggestions on any improvements that we might make after the first full year of operation.

29.4.9  Registrant Pre-Verification

All requests for registration will be verified by our registrar to ensure that they come from a legitimate representative of Amazon or our subsidiaries.  A record of the request will be kept in our on-line domain management console including the requestor's email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviours in Question 28.  We think this is very unlikely in a registry where only Amazon or its subsidiaries are registrants but we will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognise etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms “We”, “Our” and “Amazon” may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

## 30(a). Security Policy: Summary of the security policy for the proposed registry

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions.   The .MUSIC registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

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 .MUSIC 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 .MUSIC
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 .MUSIC 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

There are no increased security levels specific for .MUSIC. However, 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.

### 30.(a).4 Commitments and Security Levels

The .MUSIC 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

# New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

## String: SONG

## Originally Posted: 13 June 2012

## Application ID: 1-1317-53837

# Applicant Information

## 1. Full legal name

```
Amazon EU S.à r.l.
```

## 2. Address of the principal place of business

Contact Information Redacted

## 3. Phone number

Contact nformation Redacted

## 4. Fax number

Contact Information Redacted

## 5. If applicable, website or URL

http://www.amazon.com/

## Primary Contact

### 6(a). Name

Ms. Lorna Jean Gradden

### 6(b). Title

Operations Director

### 6(c). Address

### 6(d). Phone Number

Contact nformation Redacted

### 6(e). Fax Number

Con ac nforma ion Redac ed

### 6(f). Email Address

Contact Information Redacted

## Secondary Contact

### 7(a). Name

Ms. Dana Brown Northcott

### 7(b). Title

Associate General Counsel, IP

### 7(c). Address

### 7(d). Phone Number

Contact  nformation Redacted

### 7(e). Fax Number

Contact  nformation Redacted

### 7(f). Email Address

Contact Informat on Redacted

## Proof of Legal Establishment

### 8(a). Legal form of the Applicant

Corporation (Société à responsabilité limitée)

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

Luxembourg

### 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.

Amazon Europe Holding Technologies S.C.S. (AEHT) owns 100% of Amazon EU S.à r.l.  AEHT is held by one unlimited partner, Amazon Europe Holdings, Inc. and two limited partners, Amazon.com, Inc. and Amazon.com Int’l Sales, Inc.

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

Amazon EU S.à r.l. is not a joint venture.

# Applicant Background

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Amazon Europe Holding Technologies S.C.S. | 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.

SONG

## 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.

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

## 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.

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the .SONG registry is:
To provide a unique and dedicated platform for Amazon while simultaneously protecting the integrity of its brand and reputation.
A .SONG registry will:

- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

## 18(b). How do you expect that your proposed gTLD will benefit registrants, Internet

## users, and others?

The .SONG registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?

Amazon intends for its new .SONG gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The .SONG registry will be run in line with current industry standards of good registry practice.

What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?

Amazon values the opportunity to be one of the first companies to own a gTLD. A .SONG registry will:

- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

What goals does your proposed gTLD have in terms of user experience?

Amazon intends for its new .SONG gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.

Provide a complete description of the applicant’s intended registration policies in support of the goals above

Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a .SONG domain name, and (iii) the dispute resolution policies for the .SONG gTLD. Amazon will continually update the Domain Management Policy as needed to reflect Amazon’s business goals and, where appropriate, ICANN consensus policies.

Registration of a domain name in the .SONG registry will be undertaken in four steps: (i) Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration. All domains in the .SONG registry will remain the property of Amazon.

For example, on the rules of eligibility, each applied for character string must conform to the .SONG rules of eligibility. Each .SONG name must:

- be at least 3 characters and no more than 63 characters long
- not contain a hyphen on the 3rd and 4th position (tagged domains)
- contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
- start and end with an alphanumeric character, not a hyphen
- not match any character strings reserved by ICANN
- not match any protected country names or geographical terms

Additionally:

- Internationalized domain names (IDN) may be supported in the .SONG registry at the second level.
- The .SONG registry will respect third party intellectual property rights.
- .SONG domains may not be delegated or assigned to third party organizations, institutions, or individuals.
- All .SONG domains will carry accurate and up-to-date registration records.

Amazon’s Intellectual Property group reserves the right to revoke a license to use a .SONG domain name, at any time, if any use of a .SONG domain name violates the Domain Management Policy.

Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?

Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

Describe whether and in what ways outreach and communications will help to achieve your projected benefits?

There is no foreseeable reason for Amazon to undertake public outreach or mass communication about its new gTLD registry because domains will be provisioned in line with Amazon’s business goals.

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

Amazon intends to initially provision a relatively small number of domains in the .SONG registry to support the business goals of Amazon. These initiatives should not impose social costs of any type on consumers.

How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?

Applications from Amazon and its subsidiaries for domains in the .SONG registry will be considered by Amazon’s Intellectual Property group and allocated in line with Amazon’s business goals. The .SONG registry will not be promoted by hundreds of registrars simultaneously, so there will not be multiple-applications for a particular domain.

Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).

Domains in the .SONG registry will be provisioned to support the business goals of Amazon.

Accordingly, “cost benefits” may be explored depending on the business goals of Amazon. Amazon shares the goals of enhancing customer trust and choice.
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 10 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?
The Domain Management Policy will include the costs and benefits of Amazon’s unique and dedicated platform for stable and secure online communication and interaction.

## 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.

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as “Amazon”), is committed to managing the .SONG registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement.  In the management of domain names in the .SONG registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration those country and territory names contained in the following lists:

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; and
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
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.

The process for reserving these names, and hence blocking them from registration, will be agreed to with our technical service provider Neustar.

Because the .SONG registry will be a single entity registry and for purposes which serve Amazon’s strategic business aims, the reserved names cannot be offered to Governments or other official bodies for their own use as this would conflict with the mission and purpose of the gTLD.  However, for the same reason, they will not be offered to third parties.

The .SONG registry only provides for the registration of names at the second level.  No third level domains will be delegated at the registry level.  It is consistent with GAC advice that Amazon may choose to create sub domains using country names or abbreviations at the third level.  For example, Amazon may register information.song and its internal users may create sub domains such as us.information.song or uk.information.song.

Amazon may also use a folder structure to represent country names in its URLs, while the block exists at the second level.  For example, information.song/germany or information.song/uk.

We imagine that over time, there will be demand from brand gTLDs leading to the development of a standardized process for requesting GAC review and ICANN approval for the release of country and territory names for registration by the Registry Operator when the registry is a single entity registry.  When such a process is in place, Amazon expects to apply for the release of country and territory names within .SONG.

# Registry Services

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .SONG registry. In making this decision, Amazon EU S.à r.l. 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 .SONG 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. Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .SONG registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .SONG.

- 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 .SONG 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

Amazon EU S.à r.l. 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 .SONG. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy 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

Amazon EU S.à r.l. 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 .SONG 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

Amazon EU S.à r.l. 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
Amazon EU S.à r.l. will not be offering services that are unique to .SONG.
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.

# Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

24.1 Introduction
Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .SONG Registry. Amazon EU S.à r.l. 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 .SONG 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, Amazon EU S.à r.l. 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 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 Amazon EU S.à r.l., 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 initiates 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 components 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 .SONG 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 .SONG.

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 .SONG 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 .SONG 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 .SONG 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 .SONG registry.

## 25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

Amazon EU S.à r.l.'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 Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .SONG 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.

25.4 Proprietary EPP Extensions

The .SONG 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 .SONG 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 .SONG registry is attached in the document titled “EPP Schema.”

25.5 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 .SONG registry.

## 26. Whois

26.1 Introduction

Amazon EU S.à r.l. 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. Amazon EU S.à r.l.’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 .SONG’s 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, .SONG’s 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 (www.whois.SONG). 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<br>
Nameservers<br>
Registrant, Technical and Administrative Contacts<br>
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<br>
Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates<br>
Packetshaper for source IP address-based bandwidth limiting<br>
Load balancers to distribute query load<br>
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 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.

Potential Forms of Abuse

As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois 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 .SONG 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 .SONG registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .SONG registry.

## 27. Registration Life Cycle

27.1 Registration Life Cycle

Introduction

.SONG 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 .SONG.

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 .SONG registry per the defined .SONG 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 .SONG 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 .SONG 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 .SONG 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 .SONG 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 general establishes the maximum term of a domain name to be 10 years, and Neustar recommends 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:

4. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
5. 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
6. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar’s message queue
7. 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
8. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer
9. 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 with Amazon EU S.à r.l. 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 .SONG 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 .SONG registry.

## 28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the .SONG registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar’s extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed .SONG space.

.SONG will be a single entity registry, with all domains registered to Amazon for use in pursuit of Amazon’s business goals. There will be no re-sellers in .SONG and there will be no market in .SONG domains. Amazon will strictly control the use of .SONG domains. Opportunities for abusive and malicious domain activity in .SONG are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

Illegal or fraudulent actions
Spam
Phishing
Pharming
Distribution of malware
Fast flux hosting
Botnets
Malicious hacking
Distribution of child pornography
Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.’s registry services

provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a “domain takedown” policy. Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.
Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry. Amazon EU S.à r.l., via Neustar, 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.
Abuse Point of Contact
As required by the Registry Agreement, Amazon EU S.à r.l. 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 conduct. Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in .SONG. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made. In addition, the registry services provider for .SONG, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints
Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in .SONG; (ii) reserves Amazon EU S.à r.l.’s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its .SONG Acceptable User Policy into its Registry-Registrar Agreement.
Under the .SONG Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name “on hold” rendering the domain name non-resolvable, transfer the domain name to another registrar and⁄or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.’s intention that all .SONG domain names will be registered and used by it and its Affiliates and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register .SONG domain names. Accordingly, the potential for abusive registrations and malicious conduct in the .SONG registry is expected to be limited. In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities. Below is initial Acceptable Use Policy for the .SONG registry.
.SONG Acceptable Use Policy
This Acceptable Use Policy gives the .SONG registry the ability to quickly lock, cancel, transfer or take ownership of any .SONG 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 .SONG 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 .SONG 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 .SONG registry or its partners. In all cases, the .SONG registry or its designees will alert .SONG 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: the attempt to acquire personally identifiable information by masquerading as a website other than .SONG’s own.

Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim’s computer or DNS records in DNS servers.

Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner’s consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.

Fast Flux 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 address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.

Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.

Malicious 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.

Child Pornography: the storage, publication, display and⁄or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The .SONG registry reserves the right, in 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 .SONG 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, in 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 .SONG 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 .SONG registry or any Registrar in connection with a domain name registration. The .SONG registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The .SONG registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the .SONG 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 registry’s ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the .SONG registry will place the domain on “ServerHold”. (It is unlikely the registrar will not timely act because Amazon EU S.à r.l. intends to use a single, gateway registrar with which it has a contract reflecting these policies). ServerHold removes the domain name from the .SONG zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the .SONG registry. The .SONG registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The 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 Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the .SONG Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .SONG Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, .SONG’s registry services provider, has developed and implemented an active “domain takedown” policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar/registrant relationship.

Amazon EU S.à r.l.’s restrictions on registration eligibility make it unlikely that any .SONG domains will be taken down. The .SONG registry rules are anticipated to exclude third parties beyond Amazon EU S.à r.l. and its Affiliates. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register .SONG domain names.

Neustar’s active prevention policies stem from the notion that registrants in .SONG have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by “typical” notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below, though it is important to note that .SONG will be managed as a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon’s subsidiaries. Therefore, the potential for abusive registrations and other activities that have a negative impact on Internet users is minimal. In the unlikely event that such abuse should occur, Amazon with its registry operator, Neustar, will implement the following policies and processes to manage such activities.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the .SONG registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar's internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar's operations, legal, support, engineering, and security teams for immediate response ("CERT Team"). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual's own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar's internal or external network elements are harmed in any fashion.

Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone.

The .SONG Registry will place the domain on "ServerHold" if the registrar has not acted within the 12-hour period.

ServerHold removes the domain name from the .SONG zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event with a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon's subsidiaries, that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the .SONG registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.

Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact Amazon EU S.à r.l.'s registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident. As .SONG is a Single Entity Registry using a single registrar whose work will be strictly controlled through a Service Level Agreement that includes the implementation of measures to prevent abusive registrations, the risk of evidence of abuse being compromised is minimized. Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.

Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries' TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its .SONG registry. Amazon EU S.à r.l. and/or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such 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 Amazon EU S.à r.l. and/or Neustar for rapid resolution of the request.

If the request involves any of the activities that can be validated by the registry and/or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .SONG registry will place the domain on "ServerHold" if the registrar has not acted within the 12-hour period.

28.3 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 often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the .SONG registry has written evidence of actual abuse of orphaned glue, the .SONG registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.

In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The .SONG registry will implement several measures to promote Whois accuracy.

Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.’s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The Amazon EU S.à r.l.’s registrar will also be charged with regularly checking Whois accuracy.

Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the Amazon EU S.à r.l. registrar who will have a contractual duty to comply with Amazon EU S.à r.l.’s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.’s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.’s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN’s Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN’s Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Only Amazon EU S.à r.l. and its Affiliates will be permitted to register and use Amazon EU S.à r.l. domain names. Accordingly, the duties of the Amazon EU S.à r.l. registrar will be very limited and closely defined. Regardless, Amazon EU S.à r.l.’s Registry-Registrar Agreement will require Amazon EU S.à r.l.’s registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the .SONG registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar 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:

Customer Support – 12 employees

Policy⁄Legal – Two employees

The resources are more than adequate to support the abuse mitigation procedures of the .SONG registry.

Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.

The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes experts in Amazon EU S.à r.l.’s registrar where one legal manager and four operational experts will be available to support Amazon EU S.à r.l.

Please note that in the above answer the terms “We”, “Our” and “Amazon” may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

## 29. Rights Protection Mechanisms

29.1 Introduction

Amazon is applying for .SONG to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.

29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon

We will closely manage this TLD by registering domains through a single registrar. Although Amazon and its subsidiaries will be the only eligible registrants, we will nonetheless require our registrar to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will remain the property of Amazon and will be provisioned to support the business goals of Amazon. Because all domains will be registered and maintained by Amazon (for use that complements our strategic business goals), we can ensure that all domains in our registries will carry accurate and up-to-date registration records.

We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.

29.2 Core measures to prevent abusive registrations

To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:

- A 30 day Sunrise process
- A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered only to Amazon or its subsidiaries through a single registrar who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.

In the very unlikely circumstances that a domain is registered and used in an improper way, we acknowledge that we will be the respondent in related proceedings and we undertake to co-operate fully with ICANN and other appropriate agencies to resolve any concerns.

29.2.1 Sunrise Eligibility

Our Sunrise Eligibility Requirements will clearly state that eligible applicants must be members of the Amazon group of companies and its subsidiaries. Furthermore, all domain names must be used to support the business goals of Amazon. Nonetheless, notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.

29.2.2 Sunrise Window

As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize “all word marks: (i) nationally or regionally 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; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008”.

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will have a one year term of registration. Any domain names registered will be managed by our registrar.

29.2.3 Sunrise Dispute Resolution Policy

We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will apply to all our registries and will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):

(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.

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by our registrar. Our registrar will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service

Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honour and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the

Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by our registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)

Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.

Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

The Implementation Team will create a formal Registry Launch plan by 1 October 2012. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will be built by 1 December 2012 or within 30 days of pre-validation testing beginning, whichever is the sooner. It will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrar (the RAA) will require that the registrar uses the TMCH, adheres to the Terms & Conditions of the TMCH and will prohibit the registrar from filing domains in our registries on its own behalf or utilizing any data from the TMCH except in the provision of its duties as our registrar.

When processing TMCS claims, our registrar will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.

We will also require our registrar to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.
- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.
- The Post Delegation Dispute Resolution Procedure (PDDRP).
- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries. As domains in our registry will be registered not to third parties but only to Amazon or its subsidiaries through a single registrar which will be required through contract to ensure that the rules covering eligibility and use of a domain are adhered to, we believe that abusive registrations by third parties should be completely prevented.

Abusive behaviour by representatives of Amazon or our subsidiaries will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrar.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints against us, as the registrant, are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith. In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

Amazon or its subsidiaries will be the respondent in all UDRP complaints because we will be the only eligible registrants. Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no rights or legitimate interests” in a domain in our registry so the possibility of good faith UDRP complaints should be minimized. In the unlikely circumstances that a complaint is made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.

We will be applying for an exemption to Clause 1b of the Registry Operators Code of Conduct. This means that we will not be allowed to transfer domains to third parties as the only registrant will be Amazon or our subsidiaries. Therefore if a complaint against us is filed, the only possible remedy will be the cancellation of the domain instead of the transfer to the complainant.

Should a successful complaint be made we will therefore place the cancelled domain that is the subject of the complaint on a list that prevents it from being registered again.

29.3.2 The URS

The URS is intended to be a lighter, quicker complement to the UDRP. Like the UDRP, it is intended for clear-cut cases of trademark abuse. Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences. Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year. Either party may file a de novo appeal within 14 days of a decision. There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

As with the description of our UDRP process above, Amazon or its subsidiaries will be the respondent in all URS complaints because we will be the only eligible registrants. Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no legitimate right or interest to the domain name” and “that the domain name was registered and is being used in bad faith.” Notwithstanding this, should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator. Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.

We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

Being the only eligible registrant, we will not make changes to a domain in Locked Status or alter a registration record associated with a URS complaint as required in the Applicant Guidebook.

29.3.3 The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse. In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms. The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarising the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant's mark or (ii) impairs the distinctive character or the reputation of the complainant's mark, or(iii) creates a likelihood of confusion with the complainant's mark.”

Whilst we will co-operate with any complaints made under the PDDRP and we will abide by any determinations, we think it is highly improbable that any PDDRP complaints will succeed because the grounds set out above cannot be satisfied as domains in the registry will not be for sale and cannot be transferred to third parties.

29.3.4 Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois. A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars). Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on our registrar to ensure that all registrations are filed with accurate Whois details and we will undertake reviews of Whois accuracy every three months to ensure that the integrity of data under our control is maintained.

Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

29.3.5 Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring our registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.
- Confirming the implementation of the lock to the relevant URS provider, and ensure our registrar confirms the implementation of the lock to the relevant UDRP provider.
- Ensuring that our registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours
- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for a registry where the only registrant is Amazon or its subsidiaries. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require our registrar to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see:
http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

## 29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

### 29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

### 29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.

An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.

The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

### 29.4.3 Registrar Accreditation

Amazon will audit the performance of our registrar every six months and re-validate our Registry-Registrar Agreements annually. Our audits will include site visits to ensure the security of data etc.

### 29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed by our registrar to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

### 29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

### 29.4.6 Click Wrapping our Terms & Conditions

Although only Amazon and its subsidiaries can register domain names in our registry, we will bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

### 29.4.7 Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website. This will include relevant statistics and it will outline all cases and how they were resolved.

### 29.4.8 Contacts with WIPO and other DRS providers

Amazon will invite representatives of WIPO and other DRS providers to review our RPM and to make suggestions on any improvements that we might make after the first full year of operation.

### 29.4.9 Registrant Pre-Verification

All requests for registration will be verified by our registrar to ensure that they come from a legitimate representative of Amazon or our subsidiaries.  A record of the request will be kept in our on-line domain management console including the requestor’s email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviours in Question 28.  We think this is very unlikely in a registry where only Amazon or its subsidiaries are registrants but we will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognise etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms “We”, “Our” and “Amazon” may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

## 30(a). Security Policy: Summary of the security policy for the proposed registry

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions.   The .SONG registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

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 .SONG 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 .SONG
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 .SONG 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

There are no increased security levels specific for .SONG. However, 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.

30.(a).4 Commitments and Security Levels

The .SONG 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

# New gTLD Application Submitted to ICANN by: Amazon EU S.à r.l.

## String: TUNES

## Originally Posted: 13 June 2012

## Application ID: 1-1317-30761

# Applicant Information

## 1. Full legal name

```
Amazon EU S.à r.l.
```

## 2. Address of the principal place of business

Contact Information Redacted

## 3. Phone number

Contact Information Redacted

## 4. Fax number

Contact  nformation Redacted

## 5. If applicable, website or URL

http:⁄⁄www.amazon.com⁄

# Primary Contact

## 6(a). Name

Ms. Lorna Jean Gradden

## 6(b). Title

Operations Director

## 6(c). Address

## 6(d). Phone Number

Con ac   nforma ion Redac ed

## 6(e). Fax Number

Contact  nformation Redacted

## 6(f). Email Address

Contact Information Redacted

# Secondary Contact

## 7(a). Name

Ms. Dana Brown Northcott

## 7(b). Title

Associate General Counsel, IP

### 7(c). Address

### 7(d). Phone Number

Contact  nformation Redacted

### 7(e). Fax Number

Contact  nformation Redacted

### 7(f). Email Address

Contact Informat on Redacted

## Proof of Legal Establishment

### 8(a). Legal form of the Applicant

Corporation (Société à responsabilité limitée)

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

Luxembourg

### 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.

Amazon Europe Holding Technologies S.C.S. (AEHT) owns 100% of Amazon EU S.à r.l.  AEHT is held by one unlimited partner, Amazon Europe Holdings, Inc. and two limited partners, Amazon.com, Inc. and Amazon.com Int’l Sales, Inc.

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

Amazon EU S.à r.l. is not a joint venture.

## Applicant Background

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Allan Lyall | Manager |
| Eric Laurent Broussard | Manager |
| Eva Charlotte Gehlin | Manager |
| Gregory William Greeley | Manager |
| John Timothy Leslie | Manager |

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

| | |
|---|---|
| Amazon Europe Holding Technologies S.C.S. | 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.

TUNES

## 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.

Neustar, Amazon EU S.à r.l.'s provider of back end registry services, confirms that it does not anticipate any problems in the operation or rendering of this ASCII string. The string conforms to accepted standards and poses no threat to the operational security and stability of the Internet.

## 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.

Founded in 1994, Amazon opened on the World Wide Web in July 1995 and today offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices. Amazon and other sellers offer millions of unique new, refurbished and used items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon Web Services provides Amazon's developer customers with access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform, which developers can use to enable virtually any type of business. The new latest generation Kindle is the lightest, most compact Kindle ever and features the same 6-inch, most advanced electronic ink display that reads like real paper even in bright sunlight. Kindle Touch is a new addition to the Kindle family with an easy-to-use touch screen that makes it easier than ever to turn pages, search, shop, and take notes – still with all the benefits of the most advanced electronic ink display. Kindle Touch 3G is the top of the line e-reader and offers the same new design and features of Kindle Touch, with the unparalleled added convenience of free 3G. Kindle Fire is the Kindle for movies, TV shows, music, books, magazines, apps, games and web browsing with all the content, free storage in the Amazon Cloud, Whispersync, Amazon Silk (Amazon's new revolutionary cloud-accelerated web browser), vibrant color touch screen, and powerful dual-core processor.

The mission of the .TUNES registry is:
To provide a unique and dedicated platform for Amazon while simultaneously protecting the integrity of its brand and reputation.
A .TUNES registry will:

- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

## 18(b). How do you expect that your proposed gTLD will benefit registrants, Internet

## users, and others?

The .TUNES registry will benefit registrants and internet users by offering a stable and secure foundation for online communication and interaction.

What is the goal of your proposed gTLD in terms of areas of specialty, service levels or reputation?
Amazon intends for its new .TUNES gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction. The .TUNES registry will be run in line with current industry standards of good registry practice.
What do you anticipate your proposed gTLD will add to the current space in terms of competition, differentiation or innovation?
Amazon values the opportunity to be one of the first companies to own a gTLD. A .TUNES registry will:

- Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.
- Provide Amazon a further platform for innovation.
- Enable Amazon to protect its intellectual property rights.

What goals does your proposed gTLD have in terms of user experience?
Amazon intends for its new .TUNES gTLD to provide a unique and dedicated platform for stable and secure online communication and interaction.
Provide a complete description of the applicant’s intended registration policies in support of the goals above
Amazon’s Intellectual Property group will be responsible for the development, maintenance and enforcement of a Domain Management Policy. The Domain Management Policy will define (i) the rules associated with eligibility and domain name allocation, (ii) the license terms governing the use of a .TUNES domain name, and (iii) the dispute resolution policies for the .TUNES gTLD. Amazon will continually update the Domain Management Policy as needed to reflect Amazon’s business goals and, where appropriate, ICANN consensus policies.
Registration of a domain name in the .TUNES registry will be undertaken in four steps: (i) Eligibility Confirmation, (ii) Naming Convention Check, (iii) Acceptable Use Review, and (iv) Registration. All domains in the .TUNES registry will remain the property of Amazon.
For example, on the rules of eligibility, each applied for character string must conform to the .TUNES rules of eligibility. Each .TUNES name must:

- be at least 3 characters and no more than 63 characters long
- not contain a hyphen on the 3rd and 4th position (tagged domains)
- contain only letters (a-z), numbers (0-9) and hyphens or a combination of these
- start and end with an alphanumeric character, not a hyphen
- not match any character strings reserved by ICANN
- not match any protected country names or geographical terms

Additionally:

- Internationalized domain names (IDN) may be supported in the .TUNES registry at the second level.
- The .TUNES registry will respect third party intellectual property rights.
- .TUNES domains may not be delegated or assigned to third party organizations, institutions, or individuals.
- All .TUNES domains will carry accurate and up-to-date registration records.

Amazon’s Intellectual Property group reserves the right to revoke a license to use a .TUNES domain name, at any time, if any use of a .TUNES domain name violates the Domain Management Policy.
Will your proposed gTLD impose any measures for protecting the privacy of confidential information of registrants or users?
Yes. Amazon will implement appropriate privacy policies respecting requirements of local jurisdictions. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.
Describe whether and in what ways outreach and communications will help to achieve your projected benefits?
There is no foreseeable reason for Amazon to undertake public outreach or mass communication about its new gTLD registry because domains will be provisioned in line with Amazon’s business goals.

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

Amazon intends to initially provision a relatively small number of domains in the .TUNES registry to support the business goals of Amazon. These initiatives should not impose social costs of any type on consumers.
How will multiple applications for a particular domain be resolved, for example, by auction or on a first come first served basis?
Applications from Amazon and its subsidiaries for domains in the .TUNES registry will be considered by Amazon’s Intellectual Property group and allocated in line with Amazon’s business goals. The .TUNES registry will not be promoted by hundreds of registrars simultaneously, so there will not be multiple-applications for a particular domain.
Explain any cost benefits for registrants you intend to implement (e.g. advantageous pricing, introductory discounts, bulk registration discounts).

Domains in the .TUNES registry will be provisioned to support the business goals of Amazon. Accordingly, “cost benefits” may be explored depending on the business goals of Amazon.  Amazon shares the goals of enhancing customer trust and choice.
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 10 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?
The Domain Management Policy will include the costs and benefits of Amazon’s unique and dedicated platform for stable and secure online communication and interaction.

## 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.

Amazon EU S.à r.l., with support of its ultimate parent company, Amazon.com, Inc. (collectively referred to in this response throughout as “Amazon”), is committed to managing the .TUNES registry in full compliance with all applicable laws, consensus policies, ICANN guidelines, RFCs and the Specifications of the Registry Agreement.  In the management of domain names in the .TUNES registry, based on GAC advice and Specification 5, Amazon intends to block from initial registration those country and territory names contained in the following lists:

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; and
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
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.

The process for reserving these names, and hence blocking them from registration, will be agreed to with our technical service provider Neustar.

Because the .TUNES registry will be a single entity registry and for purposes which serve Amazon’s strategic business aims, the reserved names cannot be offered to Governments or other official bodies for their own use as this would conflict with the mission and purpose of the gTLD.  However, for the same reason, they will not be offered to third parties.

The .TUNES registry only provides for the registration of names at the second level.  No third level domains will be delegated at the registry level.  It is consistent with GAC advice that Amazon may choose to create sub domains using country names or abbreviations at the third level.  For example, Amazon may register information.tunes and its internal users may create sub domains such as us.information.tunes or uk.information.tunes.

Amazon may also use a folder structure to represent country names in its URLs, while the block exists at the second level.  For example, information.tunes/germany or information.tunes/uk.

We imagine that over time, there will be demand from brand gTLDs leading to the development of a standardized process for requesting GAC review and ICANN approval for the release of country and territory names for registration by the Registry Operator when the registry is a single entity registry.  When such a process is in place, Amazon expects to apply for the release of country and territory names within .TUNES.

# Registry Services

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

23.1 Introduction

Amazon EU S.à r.l. has elected to partner with Neustar, Inc. to provide back-end services for the .TUNES registry. In making this decision, Amazon EU S.à r.l. 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 .TUNES 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.  Amazon EU S.à r.l. will use Neustar's Registry Services platform to deploy the .TUNES registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .TUNES.

- 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 .TUNES 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

Amazon EU S.à r.l. 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 .TUNES.  The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy 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

Amazon EU S.à r.l. 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 .TUNES 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
Amazon EU S.à r.l. 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
Amazon EU S.à r.l. will not be offering services that are unique to .TUNES.
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.

# Demonstration of Technical & Operational Capability

## 24. Shared Registration System (SRS) Performance

24.1 Introduction
Amazon EU S.à r.l. has partnered with Neustar, Inc., an experienced TLD registry operator, for the operation of the .TUNES Registry.  Amazon EU S.à r.l. 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 .TUNES 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, Amazon EU S.à r.l. 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 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 Amazon EU S.à r.l., 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 initiates 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 components 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 .TUNES 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 .TUNES.

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 .TUNES 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 .TUNES 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 .TUNES 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 .TUNES registry.

## 25. Extensible Provisioning Protocol (EPP)

25.1 Introduction
Amazon EU S.à r.l.’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 Amazon EU S.à r.l. is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .TUNES 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.

25.4 Proprietary EPP Extensions

The .TUNES 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 .TUNES 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 .TUNES registry is attached in the document titled “EPP Schema.”

25.5 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 .TUNES registry.

## 26. Whois

26.1 Introduction

Amazon EU S.à r.l. 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.  Amazon EU S.à r.l.’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 .TUNES’s 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, .TUNES’s 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 (www.whois.TUNES). 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 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.

Potential Forms of Abuse

As recognized by the Terms of Reference for Whois Misuse Studies, http://gnso.icann.org/issues/whois/tor-whois-misuse-studies-25sep09-en.pdf, a number of reported and recorded harmful acts, such as spam, phishing, identity theft, and stalking which Registrants believe were sent using WHOIS contact information. Although these Whois studies are still underway, there is a general belief that public access to Whois data may lead to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose. One of the other key focuses of these studies will be to correlate the reported incidents of harmful acts with anti-harvesting measures that some Registrars and Registries apply to WHOIS queries (e.g., rate limiting, CAPTCHA, etc.).

Neustar firmly believes that adding the increased search capabilities, without appropriate controls could exacerbate the potential abuses associated with the Whois 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 .TUNES 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 .TUNES registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .TUNES registry.

## 27. Registration Life Cycle

27.1 Registration Life Cycle

Introduction

.TUNES 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 .TUNES.

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 .TUNES registry per the defined .TUNES 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 .TUNES 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 .TUNES 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 .TUNES 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 .TUNES 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 general establishes the maximum term of a domain name to be 10 years, and Neustar recommends 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:

4. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
5. 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
6. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar’s message queue
7. 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
8. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer
9. 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 with Amazon EU S.à r.l. 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 .TUNES 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 .TUNES registry.

## 28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation

Amazon EU S.à r.l. and its registry service provider, Neustar, recognize that preventing and mitigating abuse and malicious conduct in the .TUNES registry is an important and significant responsibility. Amazon EU S.à r.l. will leverage Neustar's extensive experience in establishing and implementing registration policies to prevent and mitigate abusive and malicious domain activity within the proposed .TUNES space.

.TUNES will be a single entity registry, with all domains registered to Amazon for use in pursuit of Amazon's business goals. There will be no re-sellers in .TUNES and there will be no market in .TUNES domains. Amazon will strictly control the use of .TUNES domains. Opportunities for abusive and malicious domain activity in .TUNES are therefore very restricted but we will nonetheless abide by our obligations to ICANN. A responsible domain name registry works towards the eradication of abusive domain name registrations and malicious activity, which may include conduct such as:

Illegal or fraudulent actions

Spam

Phishing

Pharming

Distribution of malware

Fast flux hosting

Botnets

Malicious hacking

Distribution of child pornography

Online sale or distribution of illegal pharmaceuticals.

By taking an active role in researching and monitoring abusive domain name registration and malicious conduct, Neustar has developed the ability to efficiently work with various law enforcement and security communities to mitigate fast flux DNS-using botnets.

Policies and Procedures to Minimize Abusive Registrations

A registry must have the policies, resources, personnel, and expertise in place to combat such abusive registration and malicious conduct. Neustar, Amazon EU S.à r.l.'s registry services provider, has played a leading role in preventing of such abusive practices, and has developed and implemented a “domain takedown” policy.  Amazon EU S.à r.l. also believes that combating abusive use of the DNS is important in protecting registrants.

Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution. Because removing a domain name from the zone will stop all activity associated with the domain name, including websites and e-mail, the decision to remove a domain name from the DNS must follow a documented process, culminating in a determination that the domain name to be removed poses a threat to the security and stability of the Internet or the registry.  Amazon EU S.à r.l., via Neustar, 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.

Abuse Point of Contact

As required by the Registry Agreement, Amazon EU S.à r.l. 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 conduct.  Amazon EU S.à r.l. will also provide such information to ICANN before delegating any domain names in .TUNES.  This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact.  Amazon EU S.à r.l. will ensure that this information is accurate and current, and that updates are provided to ICANN if and when changes are made.  In addition, the registry services provider for .TUNES, Neustar, shall continue to have an additional point of contact for requests from registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

Amazon EU S.à r.l. will adopt an Acceptable Use Policy that (i) clearly defines the types of activities that will not be permitted in .TUNES; (ii) reserves Amazon EU S.à r.l.’s right to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy; and (iii) identify the circumstances under which Amazon EU S.à r.l. may share information with law enforcement. Amazon EU S.à r.l. will incorporate its .TUNES Acceptable User Policy into its Registry-Registrar Agreement.

Under the .TUNES Acceptable Use Policy, which is set forth below, Amazon EU S.à r.l. may lock down the domain name to prevent any changes to the domain name contact and nameserver information, place the domain name “on hold” rendering the domain name non-resolvable, transfer the domain name to another registrar  and/or in cases in which the domain name is associated with an ongoing law enforcement investigation, Amazon EU S.à r.l. will coordinate with law enforcement to assist in the investigation as described in more detail below.

It is Amazon EU S.à r.l.’s intention that all .TUNES domain names will be registered and used by it and its Affiliates and that only ICANN-accredited registrars that have signed a Registry-Registrar Agreement will be permitted to register .TUNES domain names.  Accordingly, the potential for abusive registrations and malicious conduct in the .TUNES registry is expected to be limited.  In the unlikely event that such abuse should occur, Amazon EU S.à r.l. will work with its registry services provider, Neustar, to implement the following policies and processes to prevent and mitigate such activities.  Below is initial Acceptable Use Policy for the .TUNES registry.

.TUNES Acceptable Use Policy

This Acceptable Use Policy gives the .TUNES registry the ability to quickly lock, cancel, transfer or take ownership of any .TUNES 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 .TUNES 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 .TUNES 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 .TUNES registry or its partners.   In all cases, the .TUNES registry or its designees will alert .TUNES 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:  the attempt to acquire personally identifiable information by masquerading as a website other than .TUNES’s  own.

Pharming:  the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim’s computer or DNS records in DNS servers.

Dissemination of Malware:  the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner’s consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.

Fast Flux 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 address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.

Botnetting:  the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.

Malicious 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.

Child Pornography:  the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

The .TUNES registry reserves the right, in 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 .TUNES 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, in 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 .TUNES 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 .TUNES registry or any Registrar in connection with a domain name registration. The .TUNES registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The .TUNES registry is committed to acting in a timely manner against those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy. After a complaint is received from a trusted source or third-party, or detected by the .TUNES 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 registry's ability, the sponsoring registrar will be notified and have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. If the registrar has not acted when the 12-hour period ends (i.e., is unresponsive to the request or refuses to take action), the .TUNES registry will place the domain on "ServerHold". (It is unlikely the registrar will not timely act because Amazon EU S.à r.l. intends to use a single, gateway registrar with which it has a contract reflecting these policies). ServerHold removes the domain name from the .TUNES zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

Amazon EU S.à r.l. will obtain assistance from Neustar to meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the .TUNES registry. The .TUNES registry will respond to legitimate law enforcement inquiries promptly upon receiving the request.

The 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 Amazon EU S.à r.l. for rapid resolution of the request. If the request involves any of the activities that can be validated by the registry and implicates activity covered by the .TUNES Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .TUNES Registry will place the domain on "ServerHold" if the registrar has not acted within the 12-hour period.

Monitoring for Malicious Activity

Neustar, .TUNES's registry services provider, has developed and implemented an active "domain takedown" policy in which the registry itself takes down abusive domain names.

Neustar targets domain names verified to be abusive and removes them within 12 hours regardless of whether the domain name registrar cooperated. Neustar has determined that the benefit in removing such threats outweighs any potential damage to the registrar/registrant relationship.

Amazon EU S.à r.l.'s restrictions on registration eligibility make it unlikely that any .TUNES domains will be taken down. The .TUNES registry rules are anticipated to exclude third parties beyond Amazon EU S.à r.l. and its Affiliates. Moreover, only registrars that contractually agree to cooperate in stemming abusive behaviors will be permitted to register .TUNES domain names.

Neustar's active prevention policies stem from the notion that registrants in .TUNES have a reasonable expectation that they control the data associated with their domains, especially its presence in the DNS zone. Removing a domain name from the DNS before it can cause harm is often the best preventative measure for thwarting certain malicious conduct such as botnets and malware distribution that harms not only the domain name registrant, but also potentially millions of unsuspecting Internet users.

Rapid Takedown Process

Since implementing the program, Neustar has developed two basic variations of the process. The more common process variation is a lightweight process that is triggered by "typical" notices. The less common variation is the full process that is triggered by unusual notices, which generally allege that a domain name is being used to threaten the stability and security of the TLD, or is part of a real-time investigation by law enforcement or security researchers. In these cases, accelerated action by the registry is necessary. These processes are described below, though it is important to note that .TUNES will be managed as a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon's subsidiaries. Therefore, the potential for abusive registrations and other activities that have a negative impact on Internet users is minimal. In the unlikely event that such abuse should occur, Amazon with its registry operator, Neustar, will implement the following policies and processes to manage such activities.

Lightweight Process

In addition to having an active Information Security group that, on its own initiatives, seeks out abusive practices in the .TUNES registry, Neustar is an active member in a number of security organizations that have the expertise and experience in receiving and investigating reports of abusive DNS practices, including but not limited to, the Anti-Phishing Working Group, Castle Cops, NSP-SEC, the Registration Infrastructure Safety Group and others. Each of these sources is a well-known security organization that has a reputation for preventing abuse and malicious conduct on the Internet. Aside from these organizations, Neustar also actively participates in privately run security associations that operate based on trust and anonymity, making it much easier to obtain information regarding abusive DNS activity.

Once a complaint is received from a trusted source or third-party, or detected by Neustar’s internal security group, information about the abusive practice is forwarded to an internal mail distribution list that includes members of Neustar’s operations, legal, support, engineering, and security teams for immediate response (“CERT Team”). Although the impacted URL is included in the notification e-mail, the CERT Team is trained not to investigate the URLs themselves because the URLs in question often have scripts, bugs, etc. that can compromise the individual’s own computer and the network safety. Rather, the investigation is conducted by CERT team members who can access the URLs in a laboratory environment to avoid compromising the Neustar network. The lab environment is designed specifically for these types of tests and is scrubbed on a regular basis to ensure that none of Neustar’s internal or external network elements are harmed in any fashion.

Once the complaint has been reviewed and the alleged abusive domain name activity is verified to the best of the ability of the CERT Team, the sponsoring registrar has 12 hours to investigate the activity and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone.

The .TUNES Registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

ServerHold removes the domain name from the .TUNES zone, but the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement.

Full Process

In the unlikely event with a single entity registry, whose registrants will be internal stakeholders of Amazon or Amazon’s subsidiaries, that Neustar receives a complaint that claims that a domain name is being used to threaten the stability and security of the .TUNES registry, or is a part of a real-time investigation by law enforcement or security, Neustar follows a slightly different course of action.

Upon initiation of this process, members of the CERT Team are paged and a teleconference bridge is immediately opened up for the CERT Team to assess whether the activity warrants immediate action. If the CERT Team determines the incident is not an immediate threat to the security and the stability of critical Internet infrastructure, the CERT Team provides documentation to the Neustar Network Operations Center to clearly capture the rationale for the decision and either refers the incident to the Lightweight process set forth above or closes the incident.

However, if the CERT TEAM determines that there is a reasonable likelihood that the incident warrants immediate action, a determination is made to immediately remove the domain from the zone. As such, Customer Support will contact Amazon EU S.à r.l.’s registrar immediately to communicate that there is a domain involved in a security and stability issue. The registrar is provided only the domain name in question and the broadly stated type of incident. As .TUNES is a Single Entity Registry using a single registrar whose work will be strictly controlled through a Service Level Agreement that includes the implementation of measures to prevent abusive registrations, the risk of evidence of abuse being compromised is minimized. Coordination with Law Enforcement & Industry Groups

Neustar has a close working relationship with a number of law enforcement agencies, both in the United States and Internationally. For example, in the United States, Neustar is in constant communication with the Federal Bureau of Investigation, US CERT, Homeland Security, the Food and Drug Administration, and the National Center for Missing and Exploited Children.

Neustar also participates in a number of industry groups aimed at sharing information among key industry players about the abusive registration and use of domain names. These groups include the Anti-Phishing Working Group and the Registration Infrastructure Safety Group (where Neustar served for several years on the Board of Directors). Through these organizations and others, Neustar proactively shares information with other registries, registrars, ccTLDs, law enforcement, security professionals, etc. not only on abusive domain name registrations within its own TLDs, but also with respect to information uncovered with respect to domain names in other registries’ TLDs. Neustar has often found that rarely are abuses found only in the TLDs for which it manages, but also within other TLDs, such as .com and .info. Neustar routinely provides this information to the other registries so that the relevant registry can take the appropriate action.

With the assistance of Neustar as its registry services provider, Amazon EU S.à r.l. can meet its obligations under Section 2.8 of the Registry Agreement to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its .TUNES registry. Amazon EU S.à r.l. and/or Neustar will respond to legitimate law enforcement inquiries promptly upon receiving the request. Such 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 Amazon EU S.à r.l. and/or Neustar for rapid resolution of the request.

If the request involves any of the activities that can be validated by the registry and/or Neustar and implicates the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar will have 12 hours to investigate the activity further and either (a) take down the domain name through a hold or deletion, or (b) provide the registry with a compelling argument why to keep the domain name in the zone. The .TUNES registry will place the domain on “ServerHold” if the registrar has not acted within the 12-hour period.

28.3 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 often support correct and ordinary operation of the DNS, such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the .TUNES registry has written evidence of actual abuse of orphaned glue, the .TUNES registry will act to remove those records from the zone to mitigate such malicious conduct.

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system, which serves as an umbrella protection that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system is flagged for investigation and removed if necessary. This daily DNS audit prevents not only orphaned hosts but also other records that should not be in the zone.

In addition, if either Amazon EU S.à r.l. or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification from a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The .TUNES registry will implement several measures to promote Whois accuracy.

Whois service for Amazon EU S.à r.l. will operate as follows. The registry will keep all basic contact details for each domain name in a unique internal system, which facilitates access to the domain information. In addition, Amazon EU S.à r.l. will perform internal monitoring checks and procedures that will only allow accurate Whois information and remove outdated data.

28.4.1. Authentication of Registrant Information

Amazon EU S.à r.l. will guarantee the adequate authentication of registrant data, ensuring the highest levels of accuracy and diligence when dealing with Whois data. In doing so, Amazon EU S.à r.l.'s solid internal system will undertake, but not be limited to the following measures: running checks against Whois internal records and regular verification of all contact details and other relevant registrant information. The Amazon EU S.à r.l.'s registrar will also be charged with regularly checking Whois accuracy.

Amazon EU S.à r.l. will have a well-defined registration policy that will include a requirement that complete and accurate registrant details are provided by the requestor for a domain. These details will be validated by the Amazon EU S.à r.l. registrar who will have a contractual duty to comply with Amazon EU S.à r.l.'s registration policy. The full details of every domain requestor will be kept in Amazon EU S.à r.l.'s on-line registry management dashboard which can be accessed by Amazon EU S.à r.l.'s Domain Management Team at any time.

28.4.2. Regular Monitoring of Registration Data

Amazon EU S.à r.l. will comply with ICANN's Whois requirements. Among other measures, Amazon EU S.à r.l. will regularly remind its internal personnel to comply with ICANN's Whois information Policy through regularly checking Whois data against internal records, offering Whois accuracy services, evaluating claims of fraudulent Whois data, and cancelling domain name registrations with outdated Whois details.

28.4.3. Policies and Procedures ensuring compliance

Only Amazon EU S.à r.l. and its Affiliates will be permitted to register and use Amazon EU S.à r.l. domain names. Accordingly, the duties of the Amazon EU S.à r.l. registrar will be very limited and closely defined. Regardless, Amazon EU S.à r.l.'s Registry-Registrar Agreement will require Amazon EU S.à r.l.'s registrar to take steps necessary to ensure Whois data is complete and accurate and to implement the .TUNES registration policies.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups at Neustar. The Neustar Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The Neustar Customer Service team also plays an important role in assisting with investigations, responding to customers, and notifying registrars of abusive domains. Finally, the Neustar 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:

Customer Support – 12 employees

Policy⁄Legal – Two employees

The resources are more than adequate to support the abuse mitigation procedures of the .TUNES registry.

Furthermore, Amazon EU S.à r.l. dedicates significant financial and personnel resources to combating malicious and abusive behavior in the DNS and across the internet. Amazon EU S.à r.l. will extend these resources to designating the unique abuse point of contact, regularly monitoring potential abusive and malicious activities with support from dedicated technical staff, analyzing reported abuse and malicious activity, and acting to address such reported activity.

The designated abuse prevention staff within Neustar and Amazon EU S.à r.l. will be subject to regular evaluations, receive adequate training and work under expert supervision. The abuse prevention resources will comprise both internal staff and external abuse prevention experts who would give extra advice and support when necessary. This external staff includes experts in Amazon EU S.à r.l.'s registrar where one legal manager and four operational experts will be available to support Amazon EU S.à r.l.

Please note that in the above answer the terms "We", "Our" and "Amazon" may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent, or sometimes NeuStar, the registry services provider.

## 29. Rights Protection Mechanisms

29.1 Introduction
Amazon is applying for .TUNES to provide a dedicated platform for stable and secure online communication and interaction. Amazon has several thousand registered intellectual property assets of all types including trademarks, designs, and domain names – we place the protection of our intellectual property as a high priority and we respect the intellectual property of others.

29.1.1 Rights protection in gTLD registry operation is a core objective of Amazon
We will closely manage this TLD by registering domains through a single registrar. Although Amazon and its subsidiaries will be the only eligible registrants, we will nonetheless require our registrar to work with us on a four-step registration process featuring: (i) Eligibility Confirmation; (ii) Naming Convention Check; (iii) Acceptable Use Review; and (iv) Registration. As stated in our answer to Question 18, all domains in our registry will remain the property of Amazon and will be provisioned to support the business goals of Amazon. Because all domains will be registered and maintained by Amazon (for use that complements our strategic business goals), we can ensure that all domains in our registries will carry accurate and up-to-date registration records.

We believe that the above registration process will ensure that abusive registrations are prevented, but we will continue to monitor ICANN policy developments, and update our procedures as required.

29.2 Core measures to prevent abusive registrations
To further prevent abusive registration or cybersquatting, we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated for new gTLD operators by ICANN:

- A 30 day Sunrise process
- A 60 day Trademark Claims process

Generally, these RPMs are targeted at abusive registrations undertaken by third parties. However, domains in our registry will be registered only to Amazon or its subsidiaries through a single registrar who will be contractually required to ensure that stated rules covering eligibility and use of a domain are adhered to through a validation process. As a result, abusive registrations should be prevented.

In the very unlikely circumstances that a domain is registered and used in an improper way, we acknowledge that we will be the respondent in related proceedings and we undertake to co-operate fully with ICANN and other appropriate agencies to resolve any concerns.

29.2.1 Sunrise Eligibility
Our Sunrise Eligibility Requirements will clearly state that eligible applicants must be members of the Amazon group of companies and its subsidiaries. Furthermore, all domain names must be used to support the business goals of Amazon. Nonetheless, notice of our Sunrise will be provided to third party holders of validated trademarks in the Trademark Clearinghouse as required by ICANN. Our Sunrise Eligibility Requirements will be published on the website of our registry.

29.2.2 Sunrise Window
As required in the Applicant Guidebook in section 7.1, our Sunrise window will recognize “all word marks: (i) nationally or regionally 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; or (ii) that have been court-validated; or (iii) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008”.

Our Sunrise window will last for 30 days. Applications received from an ICANN-accredited registrar will be accepted for registration if they are (i) supported by an entry in the Trademark Clearinghouse (TMCH) during our Sunrise window and (ii) satisfy our Sunrise Eligibility Requirements. Once registered, those domain names will have a one year term of registration. Any domain names registered will be managed by our registrar.

29.2.3 Sunrise Dispute Resolution Policy
We will devise and publish the rules for our Sunrise Dispute Resolution Policy (SDRP) on our registry website. Our SDRP will apply to all our registries and will allow any party to raise a challenge on the following four grounds as required in the Applicant Guidebook (6.2.4):

(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.

Complaints can be submitted through our registry website within 30 days following the closure of the Sunrise, and will be initially processed by our registrar. Our registrar will promptly report to us: (i) the challenger; (ii) the challenged domain name; (iii) the grounds upon which the complaint is based; and (iv) why the challenger believes the grounds are satisfied.

29.2.4 Trademark Claims Service
Our Trademark Claims Service (TMCS) will run for a 60 day period following the closure of our 30 day Sunrise. Our TMCS will be supported by the Trademark Clearinghouse and will provide a notice to third parties interested in filing a character string in our registry of a registered trademark right that matches the character string in the TMCH.

We will honour and recognize in our TMCS the following types of marks as defined in the Applicant Guidebook section 7.1: (i) nationally or regionally registered; (ii) court-validated; or (iii) specifically protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion.

Once received from the TMCH, with which our registry provider will interface, a claim will be initially processed by our registrar who will provide a report to us on the eligibility of the applicant.

29.2.5 Implementation and Resourcing Plans of core services to prevent abusive registration

Our Sunrise and IP Claims service will be introduced with the following timetable:

Day One: Announcement of Registry Launch and publication of registry website with details of the Sunrise and Trademark Claim Service (“TMCS”)

Day 30: Sunrise opens for 30 days on a first-come, first served basis. Once registrations are approved, they will be entered into the Shared Registry System (SRS) and published in our Thick-Whois database.

Day 60-75: Registry Open, domains applied for in the Sunrise registered and TMCS begins for a minimum of 60 days

Day 120-135: TMCS ends; normal operations continue.

Our Implementation Team will comprise the following:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development ⁄ Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years’ experience with implementing registry launches including rights protection schemes such as the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

The Implementation Team will create a formal Registry Launch plan by 1 October 2012. This plan will set out the exact process for the launch of each Amazon registry and will define responsibilities and budgets. The Registry website, which is budgeted for in the three year plans provided in our answers to Question 46, will be built by 1 December 2012 or within 30 days of pre-validation testing beginning, whichever is the sooner. It will feature Rules of Registration, Rules of Eligibility, Terms & Conditions of Registration, Acceptable Use Policies as well as the Rules of the Sunrise, the Rules of the Sunrise Dispute Resolution Policy and the Rules of the Trademark Claims Service.

Technical implementation between the registry and the Trademark Clearinghouse will be undertaken by the registry service provider as soon as practical after the Trademark Clearinghouse is operational and announces its integration process.

As demonstrated in our answer to question 46, a budget has been set aside to pay fees charged by the Trademark Clearinghouse Operator for this integration.

The contract we have with our registrar (the RAA) will require that the registrar uses the TMCH, adheres to the Terms & Conditions of the TMCH and will prohibit the registrar from filing domains in our registries on its own behalf or utilizing any data from the TMCH except in the provision of its duties as our registrar.

When processing TMCS claims, our registrar will be required to use the specific form of notice provided by ICANN in the Applicant Guidebook.

We will also require our registrar to implement appropriate privacy policies reflecting local requirements. For example, Amazon is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.

29.3 Mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

To prevent the abusive use of registered domain names on an ongoing basis we will adopt the following Rights Protection Mechanisms (RPMs) which have been mandated by ICANN:

- The Uniform Dispute Resolution Policy (UDRP) to address domain names that have been registered and used in bad faith in the TLD.
- The Uniform Rapid Suspension (URS) scheme which is a faster, more efficient alternative to the Uniform Dispute Resolution Policy to deal with clear-cut cases of cybersquatting.
- The Post Delegation Dispute Resolution Procedure (PDDRP).
- Implementation of a Thick WHOIS making it easier for rights holders to identify and locate infringing parties.

The UDRP and the URS are targeted at abusive registrations undertaken by third parties and the PDDRP at so called “Bad Actor” registries. As domains in our registry will be registered not to third parties but only to Amazon or its subsidiaries through a single registrar which will be required through contract to ensure that the rules covering eligibility and use of a domain are adhered to, we believe that abusive registrations by third parties should be completely prevented.

Abusive behaviour by representatives of Amazon or our subsidiaries will be prevented by our internal processes, for example the pre-registration validation checks and monitoring of use of our registrar.

We acknowledge that we are subject to the UDRP, the URS and the PDDRP and we will co-operate fully with ICANN and appropriate registries in the unlikely circumstances that complaints against us, as the registrant, are made.

29.3.1 The Uniform Dispute Resolution Policy (UDRP)

The UDRP is an out-of-court dispute resolution mechanism for trademark owners to resolve clear cases of bad faith, abusive registration and use of domain names. The UDRP applies by contract to all domain name registrations in gTLDs. Standing to file a UDRP complaint is limited to trademark owners who must demonstrate their rights. To prevail in a UDRP complaint, the complainant must further demonstrate that the domain name registrant has no rights or legitimate interests in the disputed domain name, and that the disputed domain name has been registered and is being used in bad faith.  In the event of a successful claim, the infringing domain name registration is transferred to the complainant’s control.

Amazon or its subsidiaries will be the respondent in all UDRP complaints because we will be the only eligible registrants. Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no rights or legitimate interests” in a domain in our registry so the possibility of good faith UDRP complaints should be minimized.  In the unlikely circumstances that a complaint is made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator.

We will be applying for an exemption to Clause 1b of the Registry Operators Code of Conduct. This means that we will not be allowed to transfer domains to third parties as the only registrant will be Amazon or our subsidiaries.  Therefore if a complaint against us is filed, the only possible remedy will be the cancellation of the domain instead of the transfer to the complainant.

Should a successful complaint be made we will therefore place the cancelled domain that is the subject of the complaint on a list that prevents it from being registered again.

### 29.3.2  The URS

The URS is intended to be a lighter, quicker complement to the UDRP.  Like the UDRP, it is intended for clear-cut cases of trademark abuse.  Under the URS, the only remedy which a panel may grant is the temporary suspension of a domain name for the duration of the registration period (which may be extended by the prevailing complainant for one year, at commercial rates). URS substantive criteria mirror those of the UDRP but with a higher burden of proof for complainants, and additional registrant defences.  Once a determination is rendered, a losing registrant has several appeal possibilities from 30 days up to one year.  Either party may file a de novo appeal within 14 days of a decision.  There are penalties for filing “abusive complaints” which may result in a ban on future URS filings.

As with the description of our UDRP process above, Amazon or its subsidiaries will be the respondent in all URS complaints because we will be the only eligible registrants.  Therefore we do not anticipate that there are any circumstances in which complainants can argue that we have “no legitimate right or interest to the domain name” and “that the domain name was registered and is being used in bad faith.”  Notwithstanding this, should a complaint be made, we will respond in a timely fashion, reflecting our contractual responsibility to ICANN as a registry operator. Should a successful complaint be made, we will suspend the domain name for the duration of the registration period.

We will co-operate with the URS panel providers and panelists as we will co-operate with UDRP panel providers and panelists.

Being the only eligible registrant, we will not make changes to a domain in Locked Status or alter a registration record associated with a URS complaint as required in the Applicant Guidebook.

### 29.3.3  The Post-Delegation Dispute Resolution Procedure (PDDRP)

The PDDRP is an administrative option for trademark owners to file an objection against a registry whose “affirmative conduct” in its operation or use of its gTLD is alleged to cause or materially contribute to trademark abuse.  In this way, the PDDRP is intended to act as a higher-level enforcement tool to assist ICANN compliance activities, where rights holders may not be able to continue to turn solely to lower-level multijurisdictional enforcement options in a vastly expanded DNS.

The  PDDRP involves a number of procedural layers, such as an administrative compliance review, appointment of a “threshold review panel”, an expert determination as to liability under the procedure (with implementation of any remedies at ICANN’s discretion), a possible de novo appeal and further appeal to arbitration under ICANN’s registry terms.  The PDDRP requires specific bad faith conduct including profit from encouraging infringement in addition to “the typical registration fee.”

As set out in the Applicant Guidebook in the appendix summarising the PDDRP, the grounds for a complaint on a second level registration are that, “(a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trademark infringing domain names; and (b) the registry operator’s bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant’s mark, which (i) takes unfair advantage of the distinctive character or the reputation of the complainant's mark or (ii) impairs the distinctive character or the reputation of the complainant's mark, or(iii) creates a likelihood of confusion with the complainant's mark.”

Whilst we will co-operate with any complaints made under the PDDRP and we will abide by any determinations, we think it is highly improbable that any PDDRP complaints will succeed because the grounds set out above cannot be satisfied as domains in the registry will not be for sale and cannot be transferred to third parties.

### 29.3.4  Thick Whois

As required in Specification 4 of the Registry agreement, all Amazon registries will provide Thick Whois.  A Thick WHOIS provides a centralized location of registrant information within the control of the registry (as opposed to thin Whois where the data is dispersed across registrars). Thick Whois will provide rights owners and law enforcement with the ability to review the registration record easily.

We will place a requirement on our registrar to ensure that all registrations are filed with accurate Whois details and we will undertake reviews of Whois accuracy every three months to ensure that the integrity of data under our control is maintained.

Amazon will create and publish a Whois Query email address so that third parties can submit queries about any domains in our registry.

### 29.3.5  Implementation and Resourcing Plans for mechanisms to identify and address the abusive use of registered domain names on an ongoing basis

Our post-launch rights protection mechanisms will be in place from Day One of the launch of the registry.

To ensure that we are compliant with our obligations as a registry operator, we will develop a section of our registry website to assist third parties involved in UDRP, URS and PDDRP complaints including third parties wishing to make a complaint, ICANN compliance staff and the providers of UDRP and URS panels. This will feature an email address for enquiries relating to disputes or seeking further information on specific domains. We will monitor this address for all of the following: Notice of Complaint, Notice of Default, URS Determination, UDRP Determination, Notice of Appeal and Appeal Panel Findings where appropriate.

As stated in our answer to Question 18, Amazon's Intellectual Property group will be responsible for the development, maintenance and enforcement of the Domain Management Policy. This will include ensuring that the following implementation targets are met:

- Locking domains that are the subject of URS complaints within 24 hours of receipt of a URS complaint, and ensuring our registrar locks domains that are the subject of UDRP complaints within 24 hours of receipt of a UDRP complaint.
- Confirming the implementation of the lock to the relevant URS provider, and ensure our registrar confirms the implementation of the lock to the relevant UDRP provider.
- Ensuring that our registrar cancels domain names that are the subject of a successful UDRP complaint within 24 hours
- Redirecting servers to a website with the ICANN mandated information following a successful URS within 24 hours

The human resources dedicated to managing post-launch RPM include:

From Amazon: the Director of IP will lead a team of up to seven experts with experience of domain name management and on-line legal dispute resolution, with access to other teams in Amazon Legal if required.

From NeuStar, registry service provider to Amazon: A Customer Support team of 12, a Product Management Team of four and a Development / Engineering Team of 19 will be available as required to support the legal team, led by Jeff Neuman. This team has over 10 years' experience with implementing registry launches including rights protection schemes including the .biz Sunrise and IP Claims.

In addition, Amazon will be supported by its Registrar which will provide two legal specialists, four client managers and six operational staff. The operational staff will undertake the validation checks on registration requests.

We are confident that this staffing is more than adequate for a registry where the only registrant is Amazon or its subsidiaries. Of course, should business goals change requiring more resources, Amazon will closely review any expansion plans, and plan for additional financial, technical, and team-member support to put the Registry in the best position for success.

We will also require our registrar to implement appropriate privacy policies reflecting the high standards that we operate. For information on our Privacy Policies, please see: http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

29.4 Additional Mechanism that exceed requirements

Rights protection is at the core of Amazon's objective in applying for this registry. Therefore we are committed to providing the following additional mechanisms:

29.4.1 Registry Legal Manager

Amazon will appoint a Legal Manager to ensure that we are compliant with ICANN policies. The Legal Manager will also handle all disputes relating to RPMs. This will involve evaluating complaints, working with external legal counsel and law enforcement, and resolving disputes. The Legal Manager will also liaise with external stakeholders including URS and UDRP panel providers, the TMCH operator and trademark holders as needed.

29.4.2 Rights Protection Help Line

Amazon will maintain a Rights Protection Help Line. Calls to this line will be allocated a Case Number and the following details will be recorded: (i) the contact details of the complainant; (ii) the domain name that is the subject of the complaint or query; (iii) the registered right, if any, that is associated with the request; and (iv) an explanation of the concerns.

An initial response to a query or complaint will be made within 24 hours. The Rights Protection Help Line will be in place on Day One of the registry. The cost of the Rights Help Line is reflected in the Projections Templates provided at Question 46 as part of on-going registry maintenance costs.

The aim of the Rights Protection Help Line is to assist third parties in understanding the mission and purpose of our registry and to see if a resolution can be found that is quicker and easier than the filing of a UDRP or URS complaint.

The Legal Manager will oversee the Rights Protection Help Line.

29.4.3 Registrar Accreditation

Amazon will audit the performance of our registrar every six months and re-validate our Registry-Registrar Agreements annually. Our audits will include site visits to ensure the security of data etc.

29.4.4 Audits of registration records

Every three months, whichever is the most of 250 or 2% of the total of domain names registered in that period will be reviewed by our registrar to ensure accurate registration records and use that is compliant with our Acceptable Use guidelines.

29.4.5 Maintenance of Registry Website

Amazon will create a website for all our registries and we will make it easy for third parties including representatives of law enforcement to contact us by featuring our full contact details (physical, email address and phone number).

29.4.6 Click Wrapping our Terms & Conditions

Although only Amazon and its subsidiaries can register domain names in our registry, we will bring to the attention of requestors of domain names the Terms & Conditions of registration and, especially, Acceptable Use terms through Click Wrapping.

29.4.7 Annual Report

Amazon will publish an Annual Report on Rights Protection in our registries on our Registry Website. This will include relevant statistics and it will outline all cases and how they were resolved.

29.4.8 Contacts with WIPO and other DRS providers

Amazon will invite representatives of WIPO and other DRS providers to review our RPM and to make suggestions on any improvements that we might make after the first full year of operation.

29.4.9 Registrant Pre-Verification

All requests for registration will be verified by our registrar to ensure that they come from a legitimate representative of Amazon or our subsidiaries. A record of the request will be kept in our on-line domain management console including the requestor’s email address and other contact information.

29.4.10 Take down Procedures

Amazon has described Takedown Procedures for domains supporting Abusive Behaviours in Question 28. We think this is very unlikely in a registry where only Amazon or its subsidiaries are registrants but we will reserve the right to terminate a registration and to take down all associated services after a review by our Legal Manager if a takedown for reasons of rights protection is requested by law enforcement, a representative of a court we recognise etc.

29.4.11 Speed of Response

Wherever possible, as outlined above, Amazon committed to a response within 24 hours of a complaint being made. This exceeds the guidelines for the UDRP and the URS.

Please note that in the above answer the terms “We”, “Our” and “Amazon” may refer to either the applicant Amazon EU S.à r.l. or Amazon.com Inc., the ultimate parent.

## 30(a). Security Policy: Summary of the security policy for the proposed registry

Amazon EU S.à r.l. and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .TUNES registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

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 .TUNES 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 .TUNES
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 .TUNES 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

There are no increased security levels specific for .TUNES. However, 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.
30.(a).4  Commitments and Security Levels
The .TUNES 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