ATTACHMENT 1
(IO Objection)

![ICC logo] International Chamber of Commerce — *The world business organization*

International Centre for Expertise   Centre international d'expertise

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

OBJECTION FORM TO BE COMPLETED BY THE OBJECTOR

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

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 This form may not be published or used for any purpose other than the proceedings pursuant to the New GTLD Dispute Resolution Procedure from ICANN administered by the ICC International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

References to use for the Procedural Documents

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

Identification of the Parties, their Representatives and related entities

Objector

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

Objector's Representative(s)

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

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

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

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

Applicant

Name	Ruby Pike, LLC
Contact	Daniel Schindler
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Other Relevant Entities

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

Add separate tables for any additional relevant related entity

Disputed gTLD

gTLD Objector objects to [.example]

Name	.Hospital (Application ID: 1-1505-15195)

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

Objection

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

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

or

[ ] **Community Objection**: there is substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.

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

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

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

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

The Guidebook further states that "[i]n light of the public interest goal noted above, the IO shall not object to an application unless at least one comment in opposition to the application is made in the public sphere." In the present case this condition has been fulfilled: several public comments in opposition have been submitted to ICANN.[1]

According to Section 3.2.5 of the Guidebook "the IO must be and remain independent and unaffiliated with any of the gTLD applicants". The IO reassures that he has no link with any of the Applicants having applied for any gTLD during the current Program. Moreover, the IO declares that he has not discussed any of the Applications for any gTLD with anyone except for the members of his Legal Team. All of this is equally true for the latter. The IO considers himself to be impartial and independent as required under the Guidebook; he confirms that he is acting in no other interest but the best interests of the public who use the global Internet.

---

[1] https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments, select string: HOSPITAL

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

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

1. The present Application for .Hospital has been submitted by Ruby Pike, LLC. According to the information supplied by the Applicant, the "parent applicant" for this TLD is Dozen Donuts, LLC (in the Application, at question 18 (a) the Applicant states that Donuts Inc. is the parent Applicant; hereafter the IO will refer to the Applicant as "Donuts"), which company "intends to increase competition and consumer choice at the top level".[2] In its role of parent Applicant Donuts has submitted over 300 Applications for a wide range of new TLD's.

2. The stated Donuts' intention for this TLD is "to serve the international community by bringing new users online through opportunities for economic growth, increased productivity, the exchange of ideas and information and greater self-expression".[3]

3. As mentioned above a number of Public Comments have been submitted to ICANN.

4. The IO decided to file the present objection against the Application for .Hospital on the ground of *Limited Public Interest* as provided by Article 3.2.1 of the Guidebook.

1.   Statement of the Ground upon which the Objection is being filed

5. According to the first paragraph of Section 3.5.3. of the Guidebook the question to be considered when a *Limited Public Interest Objection* is raised is "whether the applied-for gTLD string is contrary to general principles of international law for morality and public order". The Guidebook, then, provides a non-exhaustive list of international legal instruments (mainly human rights treaties and related instruments) holding such general principles. Also, the Guidebook, stipulates that

> "Under these principles, everyone has the right to freedom of expression, but the exercise of this right carries with it special duties and responsibilities. Accordingly, certain limited restrictions may apply."

6. The grounds against which a *Limited Public Interest Objection* needs to be tested are listed as follows:

---

[2] Application, point 18 (a), first paragraph
[3] *Ibid.*

- Incitement to or promotion of violent lawless action;

- Incitement to or promotion of discrimination based upon race, color, gender, ethnicity, religion or national origin, or other similar types of discrimination that violate generally accepted legal norms recognized under principles of international law;

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

- A determination that an applied-for gTLD string would be contrary to specific principles of international law as reflected in relevant international instruments of law.

The current Objection is exclusively based upon the fourth of these grounds.

7. In accordance with the final paragraph of the Guidebook the objections raised are based on the applied-for gTLD string itself in context with the appreciation of the stated intended purpose as it may be derived from the description of its position the Applicant has provided, especially in the section "Mission/Purpose" (Section 18) in the Application form.

2. Detailed Explanation of the Validity of the Objection and why the Objection should be upheld

General Considerations

8. Obviously, the aim of an applicant submitting an Application for a .Hospital TLD is to reach out worldwide to the public at large as well as to public and private actors and institutions operating in the hospital sector. The Applicant has itself recognized that the TLD is "attractive to registrants with a connection to hospitals and medical treatment centers around the world."[4]

9. Hospitals are an essential central part of any health care system. They play a significant role in the accomplishment of the public interest mission of public health. Their general mission is to provide medical services to the public, and to generate information for research and education concerning health related issues. To this end, they employ highly qualified and often specialized medical professionals and medical equipment in a highly organized structure and offer inpatient care. The World Health Organization (WHO) describes the role and importance of hospitals in the following way:

> "Hospitals play an important role in the health care system. They are health care institutions that have an organized medical and other professional staff, and inpatient

---

[4] Application, point 18 (a).

facilities, and deliver medical, nursing and related services 24 hours per day, 7 days per week.
Hospitals offer a varying range of acute, convalescent and terminal care using diagnostic and curative services in response to acute and chronic conditions arising from diseases as well as injuries and genetic anomalies. In doing so they generate essential information for research, education and management."

10. Hospitals are inextricably connected to health. They are an essential and indispensable part of the goods, services and facilities that are necessary for the effective fulfillment of the right to health. Therefore the IO's appreciation of a .Hospital TLD is directly connected to the concept of health.

11. Health is not just another commodity. Health is a crucial, existential need for each and every human being not seldom defining the difference between life and death. It is precisely for this reason that under international law health is recognized as a fundamental human right with a corresponding obligation to respect, protect and fulfill this human right, which is primarily entrusted to States and to intergovernmental organizations such as the United Nations. At the same time this responsibility is not exclusively reserved for these public entities. The Parties adopting the International Covenant on Economic, Social and Cultural Rights explicitly considered that "the individual, having duties to other individuals and to the community to which he belongs, is under a responsibility to strive for the promotion and observance of the rights recognized in the present Covenant".[5] Below, the IO will discuss the Covenant at greater length.

12. As early as 1948, with the proclamation of the Universal Declaration of Human Rights the General Assembly of the United Nations declared "health" to be part of this listing of Human Rights:

"Everyone has the right to a standard of living adequate for the health and well being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control." (Article 25, first paragraph)[6]

13. Since then, numerous instruments of international law confirming the human rights-status of "health" have been adopted among them, most notably, the International Covenant on Economic, Social and Cultural Rights.[7] The present objection will focus on the provisions

---

[5] International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, *Treaty Series*, Vol. 993, No. I-14531, p. 3, preamble.
[6] United Nations, General Assembly, Resolution 217 A, *Universal Declaration of Human Rights*, 10 December 1948.
[7] See also: Article 5 (e) (iv) of the 1965 International Convention on the Elimination of All Forms of Racial Discrimination; Articles 11 (1)(f) and 12 of the 1979 Convention on the Elimination of All Forms of Discrimination against Women; Article 24 of the 1989 Convention on the Rights of the Child; Article 25 of the 2006 Convention on the Rights of Persons with Disabilities. Also, the 1961 European Social Charter as revised (art. 11), the 1981 African Charter on Human and Peoples» Rights (art. 16) and the 1988 Additional Protocol to the American

of the Covenant, but this may not be interpreted as an exclusion of the other international instruments as listed in the previous footnote. All of those apply *mutatis mutandis* similarly in the present context and are part of the "specific principles of international law as reflected in relevant international instruments of law" that form the basis for this Objection.

14. The first paragraph of Article 12 of the Covenant provides that the "States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health". Paragraph 2 of this same provision lists under (d) the "creation of conditions which would assure to all medical service and medical attention in the event of sickness" as one of the obligations of States in order to assure the right to health. The Committee on Economic, Social and Cultural Rights[8] has provided the most authoritative interpretation of the Right to Health in its General Comment No. 14.[9] The Committee sets out to state in paragraph 1:

> "Health is a fundamental human right indispensable for the exercise of other human rights. Every human being is entitled to the enjoyment of the highest attainable standard of health conducive to living a life in dignity."

15. In order to comply with the legal obligations that flow from these instruments of international law States across the world are, in the service of public interest and to the best of their abilities, regulating daily life by passing laws and adopting treaties in the areas of health care, the environment, food and drugs security, labor law, etc. All of these efforts have in common that one of the aims of these regulating acts is to effectively protect the right to life as well as to protect the right to health. Also these efforts demonstrate the crucial role that governments are to play with respect to the fulfillment of the right to health.

16. At the international level the WHO is unquestionably the leading agency for international health related issues and as part of the United Nations system gathers 194 member States. The Organization, with regional offices in each continent, made a notable contribution to the promotion and protection of international health by developing the International Health Regulations, "an international legal instrument that is binding on 194 countries across the globe. Their aim is to help the international community prevent and respond to acute public health risks that have the potential to cross borders and threaten

---

Convention on Human Rights in the Area of Economic, Social and Cultural Rights (art. 10). Similarly, the right to health has been proclaimed by the Commission on Human Rights (Resolution 1989/11), as well as in the Vienna Declaration and Programme of Action of 1993 (World Conference on Human Rights, A/CONF.157/23).

[8] Established under ECOSOC Resolution 1985/17 of 28 May 1985 to carry out the monitoring functions assigned to the United Nations Economic and Social Council (ECOSOC) in articles 21 and 22 of the Covenant; the Committee also adopts General Comments on specific provisions of the Covenant.

[9] United Nations Committee on Economic, Social and Cultural Rights, General Comment No. 14, *The right to the highest attainable standard of health (art. 12 of the Covenant on Economic, Social and Cultural Rights),* 11 August 2000, E/C.12/2000/4.

people worldwide".[10] Also, the WHO Constitution was, after the adoption of the Universal Declaration, the first international instrument confirming health as a human right. The constitution also states that the "extension to all peoples of the benefits of medical, psychological and related knowledge is essential to the fullest attainment of health. […] Governments have a responsibility for the health of their peoples which can be fulfilled only by the provision of adequate health and social measures."[11]

17. For the above reasons and considerations, there is no doubt that the promotion and protection of international health is inherent to the due respect for generally accepted legal norms of public order that are recognized under fundamental principles of international law.

18. The United Nations Committee on Economic, Social and Cultural Rights defines the right to health as "a right to the enjoyment of a variety of facilities, goods, services and conditions necessary for the realization of the highest attainable standard of health."[12] Moreover, the Committee listed "hospitals" as one of "the underlying determinants of health, such as (…) hospitals, clinics and other health-related buildings, trained medical and professional personnel (…)"[13] and considered that in order to fulfil the right to health "States have to ensure the appropriate training of doctors and other medical personnel, the provision of a sufficient number of hospitals, clinics and other health-related facilities."[14] Also, the WHO in its framework for action on strengthening health systems defined six building blocks of a health system: quality health services, a well-performing health workforce, a well-functioning health information system, access to essential medical products and technologies, a good health financing system, and leadership and governance.[15] The United Nations Special Rapporteur on the Right to Health reconfirmed that "these are not only 'building blocks' for a health system, they are also "building blocks" for the right to the highest attainable standard of health."[16]

19. In paragraph 12 of its General Comment the Committee lists "availability" of "functioning public health and health-care facilities, goods and services", "accessibility" of "health facilities, goods and services", "acceptability" and "quality" as "interrelated and *essential elements*" (emphasis added) of the right to health, while stipulating that "accessibility includes the right to seek, receive and impart information and ideas concerning

---

[10] http://www.who.int/topics/international_health_regulations/en/.

[11] Constitution of the WHO, New York, 22 July 1945, United Nations, *Treaty Series*, Vol. 14, No. I-221, p. 185.

[12] *Op. cit.* (fn. 9), para. 9.

[13] *Ibid,* para. 12 (b).

[14] *Ibid,* para. 36.

[15] World Health Organisation, Everybody's Business: Strengthening Health Systems to Improve Health Outcomes, 2007, p. 6, available at: http://who.int/healthsystems/strategy/everybodys_business.pdf [accessed 10 March 2013].

[16] *Report of the United Nation Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Paul Hunt*, A/HRC/7/1, 31 January 2008.

health issues [and] implies that medical services (…) are within safe physical reach''. In this context the Committee observes that "(…) States should also ensure that third parties do not limit people's access to health-related information and services".[17]

20. Thus, access to health-related information as well as access to health-related facilities, goods and services are essential elements of the right to health. Clearly, any good-faith-interpretation of the meaning of the right to receive or have access to health-related information will conclude that this right implies "to receive or have access to *reliable and trustworthy* information". This is further demonstrated by the Committee where it observes that "States should refrain from (…) intentionally misrepresenting health-related information" and considers "deliberate withholding or misrepresenting of information vital to health protection or treatment" as a violation of the obligations of States under the Covenant.[18]

21. Case law of regional Human Rights Courts confirms that access to information is an essential element of specific human rights. For example, the European Court of Human Rights found that States need to actively provide information on risks to general public health. The Court ruled that the failure to provide local population with information about the risk factors related to potential accidents at a nearby chemical factory constituted a violation of the right to respect for private and family life as contained in article 8 of the Convention.[19]

22. Having access to reliable and trustworthy health-related information is part of the right to health. States providing misleading health-related information are violating their obligations under the Covenant. This again shows the crucial role that governments are to play with respect to the fulfillment of the right to health, which includes access to and availability of health facilities, goods and services. Consequently, States need to be in a position to actually play the role they are expected to play under international law.

23. Concerning the position of the private sector in this context the Committee on Economic, Social and Cultural Rights observes that the obligations to protect the right to health "(…) include, inter alia, the duties of States (…) to ensure that privatization of the health sector does not constitute a threat to the availability, accessibility, acceptability and quality of health facilities, goods and services; [and] to control the marketing of medical equipment and medicines by third parties".[20] In other words, States are under an obligation to organize and regulate the health care sector, including hospitals in order to guarantee that the health care system is effective and does not jeopardize the essential elements of the right to health.

---

[17] *Ibid.*, para. 35.
[18] *Ibid.,* respectively para. 34 and para. 50
[19] European Court of Human Rights, *Guerra and others v. Italy*, 19 February 1998, para. 60, *Reports of Judgments and Decisions* 1998-I.
[20] *Op. cit.* (fn. 9), para. 35.

24. It is clear that the implementation of the obligations discussed above may be hindered, and therefore the right to health may be compromised in case any entity would launch a .Hospital TLD without having given due consideration to the fundamental rights and related obligations that are at stake and without having considered how to include mechanisms that at all times would rather strengthen than hinder these obligations and fundamental rights.

25. Various non-governmental organizations have submitted Public Comments with respect to all four of the Applications for the .Hospital TLD.[21] Many of those express great concern about the reliability and trustworthiness of a .Hospital TLD that is run by a private enterprise. Although these Comments apparently were submitted under the heading of the Community Objection Ground the IO has taken due notice of the contents thereof in his decision to submit the present Objection since the substance of the objections expressed often refers to "public interest" and "public health" as rationale for these concerns. Clearly, given the status of "health" as a fundamental human right and of "hospitals" as a constitutive element thereof as demonstrated above, these concerns fall within the parameters set for a Limited Public Interest Objection, i.e. the applied-for string may be contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law.

26. Not only public authorities, but also the private sector have responsibilities vis-à-vis the protection of human rights. The Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises developed a set of "Guiding Principles" that were endorsed by the United Nations Human Rights Council in its Resolution 17/4 of 16 June 2011.[22] This "Protect, Respect and Remedy Framework" is based on three foundational principles: that States must protect against human rights violations by third parties through effective policies, legislation, regulations and adjudication; that business enterprises should respect human rights by avoiding the infringement of human rights and addressing adverse human rights impacts with which they are involved (principle 11); and that States must ensure access to effective remedies for those affected by business-related human rights abuse.[23] As is stated in the introduction to the "Guiding Principles" these are not about "the creation of new international law obligations but in elaborating the implications of the existing standards and practices for States and businesses".[24] According to principle 12 the duty for businesses to respect human rights

---

[21] see fn. 1
[22] United Nations, Human Rights Council, Resolution 17/4, *Human rights and transnational corporations and other business enterprises*, 16 June 2011.
[23] United Nations Office of the High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights – Implementing the 'Protect, Respect, Remedy' Framework*, HR/PUB/11/04, 2011.
[24] *Ibid.*, p. 5, para. 14.

refers to "at a minimum" the human rights listed in the International Bill of Human Rights, which includes the International Covenant on Economic, Social and Cultural Rights, as discussed above.

27. The Independent Objector is of the view that any Applicant applying for a .Hospital TLD should demonstrate awareness of its duty to see to it that this TLD is organized, set up and managed in such a way that the right to health with all of the implications discussed above, including the necessity of reliability and trustworthiness, is fully respected and, consequently, should demonstrate that this duty will be effectively and continuously implemented. In addition, the Applicant should demonstrate how, given the public interest at stake, the policies and decision-making of the Applicant will be properly connected to the public authorities, national as well as international, that are under a legal obligation to respect, protect and fulfill the right to health. These are requirements that are fully justified given the specific principles of international law as reflected in relevant international instruments of law discussed above.

28. The IO will now provide his appreciation of the present Application against the background of these general observations.

The present Application

29. As mentioned above Donuts has submitted over 300 Applications for new gTLDs, including one for .health (ID 1-1489-82287). It did so through a great number of subsidiaries that are all located on the same address.

30. The texts of those submissions all seem to be entirely identical. A brief, random selection shows that the Applications for .Bingo (ID 1-1360-70873), .Golf (ID 1-1476-38656), .Clothing (ID 1-1394-96113) and .Apartments (ID 1-1341-21066) are, indeed, entirely identical to the present one, except for two paragraphs that are part of the .Hospital Application and not of these four others:

> "The .HOSPITAL TLD will be attractive to registrants with a connection to hospitals and medical treatment centers around the world. This is a broad and diverse group, and could include health care institutions, teaching hospitals, universities, charitable organizations, medical practitioners, administrators, insurance providers, animal hospitals, and others. The TLD could usefully serve as a place for hospital support efforts, including fundraising and donation; it also can provide a forum for expression regarding hospitals and medical treatment. This widely inclusive TLD would be operated in a secure and legitimate manner."[25]

---

[25] Application, point 18 (a).

Then again, this paragraph is, quite obviously, close to being identical to its 'sister-paragraph' appearing in the Application for .Health:

".HEALTH is a TLD attractive to registrants with affinity or professional interest in the term HEALTH. Because health of the population is a matter of urgent relevance around the world, this is a utilitarian and inclusive TLD. Registrants will come from a very broad and diverse group, including medical practitioners, veterinarians, scientists and researchers, biologists, nutritionists, dieticians, fitness experts, manufacturers and others interested in promoting human and animal wellness, global public health, the eradication of disease, and healthy lifestyles. The TLD also represents a broad and inclusive place for the discussion and exchange of health-related topics. Commensurate with the positive nature of the term, .HEALTH would be operated in a highly secure and legitimate manner."[26]

31. Neither in the paragraph just cited nor elsewhere in the Application Donuts demonstrates that it is aware of the fact that health is not just another commodity such as for example clothing, golf, apartments or bingo. Nowhere in the Application Donuts demonstrates awareness of the fact that health, including "hospitals" as one of its essential elements, is not only a "term" but that it also represents a fundamental right, which involves extensive obligations for all States across the globe as well as for citizens and private enterprises.

32. The second paragraph which appears in the .Medical Application but not in Donuts affiliate Applications for .Bingo, .Golf, .Clothing and .Apartment is the following:

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

1.   For this string, to supplement the periodic audit documented above, a deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes.
2.   Exclusion of registrars with a history of poor compliance;
3.   Regular monitoring by the registry of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes; and
4.   In addition to registry-based procedures, requirements that registrars have a 24/7/365 abuse contact, and remediation and takedown processes."[27]

However, these "special" protections appear in many of the multiple Applications submitted by Donuts, like .Creditcard (ID 1-1412-63109), .Legal (ID 1-1536-79233), .Insurance (ID 1-1512-20834), .Investments (1-1521-75718) and .Law (1-1523-55821. This only confirms the signaled Donuts' lack of awareness of the specifics of a .health TLD and of health-related TLDs like the present one.

---

[26] Application for .Health (ID 1-1489-82287), point 18 (a).
[27] Application, point 18 (a).

33. Donuts claims to have "consulted with and evaluated the ideas of international law enforcement, consumer privacy advocacy organizations, intellectual property interests and other Internet industry groups to create a set of protections that far exceed those in existing TLDs".[28] Due to the fact that Donuts neither provides any insight on the extent and the content of these consultations, the existence of which seems to be implied in multiple Donuts' Applications, nor details how specific issues (presumably) raised during those consultations have been translated into specific measures, the IO cannot otherwise but conclude that the awareness mentioned in the previous paragraph is completely absent. The "Public Interest Commitments" filed by the Applicant on 6 March 2013 do not remedy the absence of effective and reliable measures to meet these concerns; they simply reiterate elements already contained in the initial Application.

34. In its response to the IO's Initial Notice concerning the .Health Application of another Donuts subsidiary, Donuts highlighted some of the aspects already contained in its Application and stated that it saw no reason whatsoever to deal with any issues raised by the IO. Donuts added that it is opposed to any form of measures other than those proposed in its Application. This constant and absolute position has also been expressed by the Applicant's parent company in its responses to GAC Early Warning concerning the .Health Application of its affiliate.[29]

35. In conclusion, the present Application does not meet the standards that have to be applied for a – from the viewpoint of public interest – highly sensitive TLD. The launch of this applied-for .Hospitals TLD would, indeed, be contrary to specific principles of international law as reflected in relevant international instruments of law.

36. Reference can also be made to the position expressed by the WHO[30] and by multiple non-governmental organizations, which position is supported by the Governments of France and Mali as is clear from their Early Warnings with respect to the .Health Applications[31]: in its letter to ICANN of 11 April 2012 the WHO has requested ICANN to postpone decisions on .Health Applications in order to allow for consultations with the global health community which may lead to a satisfactory structure of a health related TLD. Inspired by these suggestions the Independent Objector objects, in the alternative, to this Application as long as the Applicant has not – after consultation and coordination with all stakeholders of the health community, including States and competent international organisations – provided solutions for the serious objections raised above.

---

[28] *Ibid.*
[29] http://donuts.co/news/files/donuts_reply_to_france_ARCHITECT_HEALTH_HOTEL_SARL_VIN.pdf; http://donuts.co/news/files/donuts_reply_to_republic_of_mali.pdf.
[30] http://newgtlds.icann.org/en/program-status/correspondence/kieny-to-beckstrom-et-al-11apr12-en.pdf.
[31] https://gacweb.icann.org/dosearchsite.action?queryString=health&where=gacweb&startIndex=0.

Remedies Requested

(Indicate the remedies requested.)

The Independent Objector requests the Expert panel to hold that the present Objection is valid. Therefore, the Expert panel should uphold the present Objection against the .Hospital Application (ID: 1-1505-15195).

In the alternative the Independent Objector requests the Expert panel to hold that the present Objection is valid as long as the Applicant has not provided solutions for the serious objections raised above. Accordingly, the Expert panel should conditionally uphold the present Objection against the .Hospital Application (ID: 1-1505-15195).

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

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

A copy of this Objection is/was transmitted to the Applicant on 13 March 2013 by e-mail to the following address: rubypike@donuts.co

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

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

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

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

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

List and Provide description of any annex filed.

-

Date: 12 March 2013

Signature:

ATTACHMENT 2
(Ruby Pike Opposition)

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

RESPONSE FORM TO BE COMPLETED BY THE APPLICANT

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

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

References to use for the Procedural Documents

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

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

Identification of the Parties and their Representatives

Applicant

Name	Ruby Pike, LLC
Contact person	Daniel Schindler, Jon Nevett
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Objector

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

Copy the information provided by the Objector.

Applicant's Representative(s)

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

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

Applicant's Contact Address

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

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

Other Related Entities – Objector's Representatives

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

Add separate tables for any additional other related entity.

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

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

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

Disputed gTLD

gTLD Applicant has applied to and Objector objects to [.example]

Name	<.hospital> – Application ID 1-1505-15195 (ICC Case No. EXP/406/ICANN/29)

Objection

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

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

or

[ ] **Community Objection**: there is substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.

Copy the information provided by the Objector.

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

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

A.

INTRODUCTION

ICANN adopted its new gTLD program to increase choice and competition in domain names. AGB Preamble, § 1.1.2.3, and Mod. 2 Attmt. at A-1. Sharing and seeking to accomplish these same goals, Donuts has applied for the instant and other TLDs, to offer domains on subjects that otherwise may not have their own forums. *See* Nevett Dec. ¶¶ 4-6 (**Annex B**).

Applicant would make the <.hospital> registry open to all consumers, creating paths of communication more expansive than the narrow use to which Objector believes the TLD should be put. Such generic TLDs bring competition to registries, which have not experienced it in a world that has known little more than <.com>, as well as the opportunity for more consumers to enjoy the benefits of such competition. A <.hospital> gTLD in Applicant's hands represents one of a number of niche offerings in an expanding Internet "shopping mall." It gives users the choice of a specialty experience as an alternative to the sprawling "department store" environment of incumbent registries such as <.com>. Nevett Dec. ¶¶ 6, 8 (**Annex B**).

The Objection threatens these important benefits. It would close an entire segment of the Internet to the many potential uses of a common word's multiple meanings. Moreover, it has been brought by an Objector whose required independence merits consideration.

About the Objector:

The Objector is Prof. Alain Pellet, appointed by ICANN to serve as the IO for the entire new gTLD program. AGB § 3.2.5. According to the IO's website, he is "impartial and is unaffiliated with any particular Internet community." *See* http://www.independent-objector-newgtlds.org/english-version/introducing-the-independent-objector/role-of-the-independent-objector. He also specifically reasserts his independence in the Objection itself. Objn at 5.

ICANN has appointed the IO to "object to highly objectionable gTLD applications that would be contrary to the [public's] interests." AGB § 3.2.5. "The IO can file objections on Limited Public Interest and Community grounds." *Id.*

Objector has filed essentially identical objections, on both LPI and community grounds, against a number of hospital-related gTLD applications made by entities of Donuts, Applicant's ultimate parent. Including the instant Objection, they are:

String	Objn Type	Applicant	App ID	ICC Case No.
<.healthcare>	LPI	Silver Glen, LLC	1-1492-32589	EXP/405/ICANN/22
<.healthcare>	Community	Silver Glen, LLC	1-1492-32589	EXP/411/ICANN/28
<.hospital>	LPI	Ruby Pike, LLC	1-1505-15195	EXP/406/ICANN/29
<.hospital>	Community	Ruby Pike, LLC	1-1505-15195	EXP/412/ICANN/23
<.medical>	LPI	Steel Hill, LLC	1-1561-23663	EXP/407/ICANN/24
<.medical>	Community	Steel Hill, LLC	1-1561-23663	EXP/413/ICANN/30
<.health>	LPI	Goose Fest, LLC	1-1489-82287	EXP/417/ICANN/34

The IO has filed relatively few objections overall, such that Donuts' applications represent a significant proportion of them. Further, almost exclusively he has attacked only applications for health-related gTLDs. However, he has not brought objections against *all* such applications. And, he has made no objections against many other strings that could be viewed as equally "sensitive" as health – *e.g.*, children, financial topics, intellectual property, gambling and education.

The IO has background in health-related matters and with particular healthcare and policy interests. He has worked with the World Health Organization (WHO), and so acknowledges in his *curriculum vitae*. *See* Nevett Dec. ¶ 18, Ex. 3 (**Annex B**). In addition, his legal assistant, Julien Boissise, has a connection to Rosa Delgado, a consultant to WHO. Ms. Delgado appears to have advocated on behalf of the International Medical Informatics Association (IMIA) in proceedings involving the ICANN At-Large Advisory Committee (ALAC), which since has brought a community objection on IMIA's behalf against Donuts' <.health> gTLD application, ICC Case No. EXP/505/ICANN/122. *Id.* Exs. 4, 5.

Clearly, the IO has some bias that favors healthcare and hospital interests and opposes those who would provide a forum for such topics on the Internet. We do not

suggest the he has engaged in any improper conduct. However, the Panel should consider the Objection in light of his healthcare bias.

About the Respondent:

The Nevett declaration in Annex B hereto provides a great deal of information concerning Donuts, its formation, management (including their background), and Internet philosophy. To summarize briefly, Respondent is owned by Donuts, which, through Respondent and other direct and indirect subsidiaries, has applied for 307 new gTLDs representing a variety of common dictionary terms. As referenced in its applications, Donuts is a well prepared, amply resourced and highly qualified organization committed to offering consumers new and varied generic domain name alternatives through safe, stable and secure registry operations.

The Donuts team consists of industry veterans with long histories of contributing to ICANN's policymaking process, successfully launching gTLDs, building industry-leading companies, and bringing innovation, value and choice to the domain name marketplace. Donuts supports ICANN's mission to increase consumer choice and competition in the domain name industry, and to widen global participation on the Internet. It seeks to help redefine the domain name space, which has featured behemoth "department store" registries such as <.com>, and make it more akin to an Internet "shopping mall," with certain "tentpole" offerings that can be attractive to many Internet users generally, coupled with a variety of niche domain models that serve a more specific, though no less important, segment of the Internet user population.

In furtherance of this approach, Donuts has made the instant Application and others on health-related subjects to augment consumer choice, bolster competition and expand avenues of expression on the Internet – goals explicitly articulated by ICANN ijn specific connection to its new gTLD program. Objector would have this Panel obstruct these laudable aims.

Objector's Burden of Proof:

ICANN has made clear:

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

http://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf.
Objector does not satisfy that burden. He cannot do so with respect to an everyday word that Applicant offers for generic Internet use and which does not in any way implicate the severe consequences that universally accepted norms of international law condemn. Objector distorts the situation here in an effort to fit his Objection into a heightened standard that simply does not contemplate it. ICANN has established its "quick look" process to prohibit such abuses. As explained more fully immediately below, the Panel should implement it and promptly dismiss the "manifestly unfounded" Objection.

1. *Objector's Abuse of Standing Warrants "Quick Look" Dismissal.*

While "[a]nyone may file a Limited Public Interest Objection …, objectors are subject to a 'quick look' procedure designed to identify and eliminate frivolous and/or abusive objections." AGB § 3.2.2.3. In furtherance of that important gatekeeping function, an objection "found to be manifestly unfounded and/or an abuse of the right to object may be dismissed at any time." *Id.*

"The quick look is the Panel's first task." *Id.* Moreover, it constitutes "a review on the merits of the objection." *Id.* Thus, ICANN has not made the process a discretionary, procedural one. Rather, because of its liberal grant of standing, ICANN has mandated a threshold review on the merits to weed out objections that attempt to access the dispute resolution process excessively ("an abuse of the right to object") or without merit ("manifestly unfounded").

The instant Objection is manifestly unfounded because, as shown more fully below, it does not "fall within one of the categories that have been defined as the grounds for such an objection." Id. The overarching principle that the Panel "will consider" is "whether the applied-for gTLD string is *contrary* to general principles of international law for *morality and public order.*" Id. § 3.5.3 (emphases added).

The standard focuses on the *string* itself not the *applicant.* For that reason, ICANN has expressly cautioned against considering "[a]n objection that attacks the applicant, rather than the applied-for string …." *Id.* The instant Objection, however, does nothing more. Devoting the bulk of its 34 paragraphs to his view of the public interest in and fundamental right to "health" (and by extension the concept of "hospital" as a place for health treatment) the Objector criticizes the Applicant for not appearing to appreciate these concepts to the extent the Objector deems appropriate. *See* Obj. ¶¶ 27-33.

Nowhere, however, does the Objector identify anything about the *string*, or regarding how the Applicant plans to administer it, that runs *contrary* to any *specific* principle of international law. Yet, the substantive objection standard places the burden on the Objector to prove exactly that. AGB §§ 3.5, 3.5.3. As shown in greater detail below, his unsupported conclusions, regarding the Applicant's "understanding" of the vague concept of the importance of "health" (and "hospital" as a place to obtain health treatment) as a public interest, do not come close to meeting the considerable burden Objector has to prove that the string itself would violate principles of morality and public order. As so "manifestly unfounded," the Objection warrants "quick look" dismissal.

In addition to falling short of the Objector's substantive burden of proof, the attacks he levels on the Applicant can also, as ICANN explicitly points out, amount to "an abuse of the right to object." AGB § 3.2.2.3. The Objector compounds the violation by filing multiple objections against the Applicant and related parties, which ICANN also specifically identifies separately as an abuse of the objection process. Quick look dismissal likewise follows on this independent ground.

ICANN did not create these screening standards out of 'thin air.' Such protections inhere in the very principles of international law that ICANN has bound the Objector to uphold. It specifically supports its approach by reference to Article 35(3) of the European Convention on Human Rights, which renders "inadmissible any individual application … incompatible with the provisions of the Convention …, manifestly ill-founded, or an abuse of the right of application," and refers to decisions thereunder published at http://www.echr.coe.int. AGB at p. 3-7 n.2, *citing* Décision partielle sur la recevabilité de la requête no 61164/00 présentée par Gérard Duringer et autres contre la France et de la requête no 18589/02 contre la France (2003).

The Panel need look no further to discern the manifestly unfounded and abusive nature of the Objection, and dismiss it outright upon its mandatory "quick look" review. Should the Panel nevertheless desire further analysis, it appears below.

2. The Objector Fails to Carry His Burden of Proof on the Substantive Grounds of the Objection.

The burden of proof for any type of objection rests solely on the objector. *See* AGB § 3.5. To prevail, the Objection must discharge that burden and *prove* that the *string* or its

intended use, as stated in the application, runs afoul of legal strictures against the type of abhorrent conduct described in the objection standard. AGB §§ 3.5, 3.5.3. Yet, Objector fails to demonstrate that his Objection "fall[s] within one of the categories … defined as the grounds for such an objection" in subsection 3.5.3 of the Guidebook. AGB § 3.2.2.3. Also, Objector fails to show specifically that, *from a statement in the Application*, the Applicant *intends* to *operate* the TLD *in contravention* of "morality and public order." Rather, the instant Objection and its undifferentiated counterparts together "constitute harassment" and not "a legitimate defense of legal norms … under general principles of international law." *Id.*

Under the "general principles of international law for morality and public order" that provide the foundation for the limited public interest objection, "everyone has the right to freedom of expression …." AGB § 3.5.3. Only "limited restrictions may apply" to this right. *Id.* Accordingly, the *only* grounds upon which ICANN allows an applied-for gTLD string to be considered "contrary to generally accepted legal norms relating to morality and public order … recognized under principles of international law" are:

- Incitement to or promotion of violent lawless action;

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

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

- A determination that an applied-for gTLD string would be *contrary* to *specific* principles of international law as reflected in relevant international instruments of law.

Id. (emphases added). The Objector confirms that he proceeds solely upon the last-listed ground. Obj. ¶ 6 at p. 7.

Importantly, that fourth criterion does not serve as a simple 'catch-all' provision for whatever the Objector may broadly consider as vaguely "reflected" in international law codifications that he unilaterally deems "relevant." While admittedly notions such as "morality and public order" are not at all easy to pin down, even a cursory reading of the LPI standard shows the very serious nature of the topics that were contemplated when creating the objection: genocide, torture, slavery, violence against women, racism, and child pornography/sexual abuse. *See* AGB pp. 3-20 to 3-22. Further, ICANN notes in the Draft Discussion Memo that certain "peremptory norms of public international law" exits for which *no delegation is permitted*' and which can "modified only by a subsequent norm of international law having the same character (*jus cogens*)."

To the contrary, under universally accepted tenets of interpretation, the last item in the list "catches" no more than situations *like* those described in the previous three. *See, e.g.:***"Ejusdem generis ("of the same kinds, class, or nature")***

When a list of two or more specific descriptors is followed by more general descriptors, the otherwise wide meaning of the general descriptors must be restricted to the same class, if any, of the specific words that precede them. For example, where "cars, motor bikes, motor powered vehicles" are mentioned, the word "vehicles" would be interpreted in a limited sense (therefore vehicles cannot be interpreted as including airplanes).

If this universally recognized axiom of interpretation did not so clearly lead to this conclusion, ICANN itself unequivocally eliminates any ambiguity. It states the "fourth standard … in general terms" in order to give a panel the "discretion to consider gTLD strings that do not fit within one of the three *specific* categories," but only to the extent "*contrary* to generally

accepted legal norms relating to morality and public order *to the same degree* as the first three grounds. *Applications for such strings may well be rare or non-existent.*" *See* http://www.icann.org/en/topics/new-gtlds/agv2-analysis-public-comments-31may09-en.pdf In other words, the subject string must *violate* precepts of international law closely akin to those proscribing such severe *transgressions* as lawless violence, discrimination based on race or similar inborn characteristics, or child pornography and sexual abuse.

Also, while they can often be every bit as troublesome to isolate, free speech principles do carry some widely-accepted norms that can be adopted for purposes of LPI analysis, such as prohibitions on inciting violent or lawless behavior (yelling "Fire!" in a crowded theatre); disseminating hate speech or racial slurs; and similar things. Indeed, as mentioned the Guidebook even includes a specific reference to free speech and its outer boundaries (*id.* § 3.5.3).

However one defines "morality" or "public order," one cannot argue that the *string itself* — the simple word "hospital" — indicates any form of unlawful or wrongful behavior. Indeed, Objector even states in his Objection that he considers the term "hospital" as being "directly connected to the concept of health," and that the latter is a "crucial and existential need for each and every human being." *See* Objn at 7-8. Similarly, nothing suggested by the Application, to which the Objector purports to refer for context, is itself "contrary" to "morality" or "public order." In its Application, Respondent simply states a <.hospital> gTLD would be:

> attractive to registrants with affinity or professional interest in promotion or treatment of human health, and the methods of delivery and payment for health care services. This includes, but is not limited to, those engaged in the treatment and prevention of disease and illness, the provision of primary and secondary care, the dissemination of health care information, and the advancement of public health. The term is also highly topical in the global discussion of healthcare policy and administration, and is a useful forum for debate and the exchange of ideas. We would operate this TLD in the best interests of all registrants, and in a stable and secure manner."

See Obj. at 13, *quoting* Application Q18A, **Annex B** (Nevett Dec. Ex. 1 at 7-8). Maintaining a "global discussion of healthcare policy and administration" and a "useful forum for debate and the exchange of ideas" in a "stable and secure manner" would hardly seem to be against public interest. On the contrary, given that Donuts' approach is *inclusive* and not focused on content control, it would like help *facilitate* such interests through increased discourse and greater communication.

By objecting to a simple expression like "hospital," the Objector falls well short of his substantial burden. Objector offers no meaningful evidence that tends in any way to *prove* that the string *itself*, or Applicant's stated *intent* in operating it, will violate such inarguable legal norms. Rather, Objector would have the Panel simply *infer* such affirmative malicious conduct and intent entirely, and solely, from the following innocuous and amorphous factors:

- That Donuts entities have applied for over 300 new gTLDs, Obj. ¶ 28;

- That the publicly available portions of all such applications appear nearly indistinguishable, save for certain provisions by which the Applicant distinguishes the particular string applied for here, and identifies ways in which it will take into account concerns such as those expressed by the instant Objection, Obj. ¶ 29;

- That neither the common nor the unique provisions of the Application demonstrate Donuts' "awareness" that "health" (which according to the

Objector underlies the term "hospital)" is not just a "term" but also a "fundamental right," Obj. ¶ 30;

- That the "special" protections proposed in the Application also "appear in many of the multiple Applications submitted by Donuts" entities, which the Objector concludes "confirms" their lack of "awareness" of the issues specifically implicated by a <.hospital> TLD, Obj. ¶ 31;

- That Donuts entities claim in "multiple" applications to have "consulted" with international law, consumer privacy, intellectual property and other Internet industry interests, but that Applicant does not show how "specific issues" presumably raised in such consultations have "translated into specific measures" that the Objector believes should be applied here, Obj. ¶ 32;

- That the Objector's inability to determine such "specific measures" causes him to "conclude" that the Applicant's "awareness" of <.hospital> TLD issues "is completely absent," *id.*;

- That in previous interactions with the Objector (on <.health>) Applicant stated its view that the opinions he then articulated (and repeats here) do not qualify as an LPI objection; Obj. ¶ 33;

- That Applicant's "Public Interest Commitments" ("PIC"s) do not, in the Objector's view, "remedy the absence of effective and reliable measures" to meet his concerns, *id.*; and

- That the Application (in his view) does not "meet the standards" that the Objector believes "have to be applied" for a "highly sensitive" TLD such as <.hospital>, Obj. ¶ 34;

- That the World Health Organization (WHO) and "multiple non-governmental organizations," whose "position is supported by the Governments of France and Mali," has "requested ICANN to postpone decisions" on applications for a *health* TLD "in order to allow for consultations" which "may" lead to a "satisfactory structure" for such a TLD, Obj. ¶ 35.

- That certain third parties have expressed their "fears" concerning the Respondent's use of the TLD "solely" to advance its own commercial interests, Obj. ¶ 35.

Such neutral and/or unsubstantiated information — or what Objector *perceives* from it — does not even begin to satisfy Objector's heavy burden to prove that the *string* (or Applicant's *stated intent* in running it) is sufficiently likely to infringe upon international law norms against such widely despised behaviors as violence, discrimination, slavery, child pornography and the like. Objector cites not a single provision of international law to which the applied-for *string*, or anything the Applicant plans to do with it, runs *contrary*, as the substantive objection standard requires.   As additional examples:

- Whether Donuts entities have applied for three, three hundred or three thousand TLDs does not prove that the TLD applied for *here* will breach *any* international law restrictions, let alone those against the serious types of transgressions contemplated by the substantive objection standard;

- Whether the instant Application resembles or differs from the over 300 others submitted by related entities neither proves that the string does, nor demonstrates that Applicant intends to, violate widely accepted international

> law norms against violent, discriminatory, sexually abusive or similarly egregious behavior;

- What Objector perceives as Applicant's lack of "awareness" of the internationally weighty "issues" raised by a <.HOSPITAL> domain does not amount to *evidence* that the domain *will* or is *intended* to operate outside the boundaries of international laws proscribing socially unacceptable, dangerous and morally deviant behavior;

- Whether or not the Objector *perceives* Applicant's "protections" as "adequate" does not satisfy his burden of proving *affirmatively* or *intentionally* improper conduct of the extraordinary nature required merely to *state* a valid LPI objection, let alone succeed with it; and

- The "standards" that the Objector believes "have to be applied" for a so-called "highly sensitive" TLD such as <.HOSPITAL>, and the "measures" that "may" lead to what he and others deem a "satisfactory structure" for that TLD, cannot and do not substitute for the elements of LPI objections that ICANN explicitly requires and which Objector has failed to meet.

Objector's does not overcome the strong "presumption … in favor of granting new gTLDs to applicants who … satisfy the requirements for obtaining' them, as ICANN, by its Initial Review, has found this Applicant to have done. At best, all the Objector has really done in his Objection is criticize the Respondent for providing insufficient information about how it plans to mitigate potential harm. However, the Respondent *did* provide a great deal of information in its Application (*See* Respondent to Question 18(a)) and stated unequivocally that not only has it worked closely with ICANN and a variety of stakeholders (including industry experts, law enforcement, government representatives, legal professionals and others) to establish at least *fourteen* new protective measures developed by ICANN specifically   for the new gTLD program (including not only the well-known UDRP but also a "Uniform Rapid Suspension" system, the implementation of a "Trademark Clearinghouse" etc.) but has also voluntarily agreed to implement *eight additional* measures that are designed to provide an even higher level of protection to Internet users. *Id.* Finally, for certain TLDs that Donuts indicated as sensitive, including <.hospital>, Donuts also included even more protections. *See* Nevett Dec. ¶¶ 9-12 (**Annex B**).

The Panel should dismiss the Objection as "manifestly unfounded and/or an abuse of the right to object" after the requisite "quick look." It certainly should do so upon closer examination, should it choose to engage in such review.

3. The Panel Should Waste No Time and Deny the Objection for Failure to Meet its Burden.

What the Objector idealizes an LPI *should* do bears no resemblance whatsoever to what ICANN has stated it *must* do. The Guidebook was derived over years through ICANN's multi-stakeholder model with input for governments and other community members. Objector appears to be trying to replace the actual rules that were approved and relied upon with ones that he likes better. *See* Nevett Dec. ¶¶ 3-4 (**Annex B**). He may well, and understandably, view the concept of "health" as an important international issue and even a fundamental human right. However, the sole issue before this Panel is whether or not the applied-for string, or Applicant's proposed operation of it, is *contrary* to any identified provision of international law against the type of extensively reviled conduct specified in the substantive objection standard.

Indeed, it is the *Objector* who arguably infringes upon the fundamental rights of Respondent and the public to free expression. Free speech rights are not reserved for a

privileged few. The tools of free speech—today, the Internet and domain names—are logically and similarly unencumbered, and must remain so if these ideals are to be upheld.

Respondent is the only applicant for <.hospital>. If Objector somehow succeeds in his objection, the TLD will not be available for any members of the public. There would be no <.hospital> sites for citizens to discuss hospital concerns, policies or reviews of institutions. The exchange of ideas would be more limited. A very unfortunate result.

Respondent intends to operate open and unrestricted gTLDs for the benefit of all law-abiding users. The Panel should bear in mind, however, that — as is the case in all forms of progress — there may be some level of cost. Further, stakeholders should recognize the net benefit to the worldwide community and encourage expansion of the benefit, instead of closing great sections of opportunity due to perceived possible (though unlikely) harm. We must avoid choking growth and legitimate activity. The Objector's approach is to simply curtail any plans to provide competition and increased consumer choice. It would be like not permitting the building of a shopping mall simply because someone *might* engage in shoplifting, which already happens in existing department stores (and will continue to happen) in other situations, even though the zoning requirement would ensure and the builder has voluntarily committed to having more security at the new mall than at the existing stores.

In a similar vein, the Panel should also take note of the abundant use of the term "hospital" in numerous second-level domain names. Indeed, Donuts searched the root zone of six existing gTLDs, including <.com>, and found over 26,000 uses at the second of the same term that Objector here claims will run afoul of international precepts of morality and public order. Nevett Dec. ¶ 17 (**Annex B**). The Objection gravely overreaches and can do nothing about these many other uses that Applicant would be preclude from competing against if the Panel were to sustain the Objection. Clearly, it must do the opposite, and deny it.

4. Conclusion.

ICANN could not have articulated its requirements for the LPI Standard more clearly. Objector has the burden to meet them, yet has failed to do so. Consequently, his Objection cannot stand and Respondent's Application must be allowed to proceed.

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

A copy of this Response is/was transmitted to the Objector on: May 15, 2013

by email to the following addresses: courriel@alainpellet.eu; avocet@bajer.fr;

mail@danielmueller.eu; phonvanderbiesen@vdbadvocaten.eu; and

swordsworth@essexcourt.net.

A copy of this Response is/was transmitted to ICANN on May 14, 2013 by e-mail to the following addresses: newgtld@icann.org, DRfiling@icann.org.

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

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

☐ Evidence of the payment is attached for information.

Description of the Annexes filed with the Response (Article 11(e) of the Procedure)

List and Provide description of any annex filed.

Annex A – Table of Defined Terms

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

Exhibit 1 – Application ID 1-1505-15195 for <.hospital> gTLD by Ruby Pike, LLC

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

Exhibit 3 – Alain Pellet *curriculum vitae*

Exhibit 4 – February 20, 2013 Delgado email

Exhibit 5 – October 23, 2012 Delgado blog

Respectfully submitted,

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

By: _____/jmg/_____   By: _____/dcm/_____
John M. Genga   Don C. Moody
john@newgtlddisputes.com   don@newgtlddisputes.com

Attorneys for Applicant/Respondent
RUBY PIKE, LLC

May 15, 2013

Annex A

[Table of Defined Terms]

ANNEX A

Table of Defined Terms

Abbreviation	**Reference**
"ICANN"	Internet Corporation for Assigned Names and Numbers
"Guidebook" or "AGB"	The gTLD Applicant Guidebook, approved by ICANN on June 20, 2011, and as updated on January 11 and June 4, 2012
"ICC"	International Chamber of Commerce
"TLD" or "string"	A top level domain, also referred to as a "string" by ICANN – *e.g.*, Guidebook §§ 3.2.1, 3.5.4
"Objector"	Prof. Alain Pellet, Independent Objector (IO)
"Applicant" or "Respondent"	Ruby Pike, LLC
"Donuts"	Donuts Inc., ultimate parent of Applicant
"Application"	Applicant's application for the <.hospital> TLD
"Objection"	The objection to the Application submitted to the ICC by Objector on March 13, 2013
"Response"	Applicant's response to the Objection, of which this **Annex A** is a part
"Panel"	ICC's appointee to consider and rule upon the Objection

Annex B

[Declaration of Jonathon Nevett]

DECLARATION OF JONATHON NEVETT

I, Jonathon Nevett, declare as follows:

1.   I am a founder and Executive Vice President of Donuts Inc., the ultimate parent of Ruby Pike, LLC ("Applicant" or "Respondent"). Applicant has filed Application No. 1-1505-15195 (the "Application") for the generic top-level domain ("gTLD") <.hospital> (at times herein, the "Domain"). A true, correct and complete copy of the public portion of the Application is attached hereto as Exhibit 1.

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

Donuts' Background

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

New gTLD Objectives and Donuts' Philosophy

4.   From my own involvement, I understand that ICANN developed the new gTLD

program to increase competition and choice in the domain name space. Indeed, the top of the

"About" page of its new gTLD website, http://newgtlds.icann.org/en/about/program, expressly so

states. I also understand that the program's intent includes the promotion of free expression, as

supported by statements in ICANN's new gTLD Applicant Guidebook ("Guidebook") – *e.g.*,

"everyone has the right to freedom of expression," Guidebook at 3-21.

5.   Donuts joins in these aims. Through subsidiary entities such as Applicant, it has

applied for 307 new gTLDs. A complete and correct list of all new gTLDs applied for by Donuts

entities is attached hereto as Exhibit 2. These applications, along with approximately 1,600

submitted by others to ICANN, *see* http://newgtlds.icann.org/en/program-status/statistics, will

create competition among domain name registries that has not previously existed in a

landscape that has had only 22 gTLDs to this point, http://newgtlds.icann.org/en/program-

status/application-results/strings-1200utc-13jun12-en. Such competition advances the

program's goals, shared by Donuts, to expand consumer choice in the name space.

6.   Donuts has adopted a business model that it believes enhances consumer

choice more effectively than it could have achieved with a lesser number of applied-for names.

By applying for and scaling up to run a large number of new gTLDs, Donuts achieves

economies of scale that allow it to offer domains representing terms and subjects that otherwise

could not be brought to the name space economically and, consequently, would not have their

own forum. In the way of analogy, Donuts views <.com> as a large downtown "department

store" that has not had much competition. Instead of competing with <.com> by building

another department store a few blocks away, Donuts' idea is to create a "shopping mall"

environment that allows for "boutiques" to share the expanding mall space. By doing so, Donuts

can provide more consumer choice and specificity in the domain name space.

7.   The 307 gTLDs for which Donuts applied were carefully selected as subject

areas that Donuts believes will interest Internet users and involve them in the domain. Donuts

deliberately chose common words from the dictionary so that consumers could make use of the

gTLDs in accordance with the meanings they ascribe to those words. In no case did Donuts opt

for a generic term *because* it also may describe a group or serve as a trademark in other

contexts. Indeed, we understand that most dictionary terms are trademarks for something in

some jurisdiction. We studied various data sources, built and utilized algorithms, and relied on

our various industry experiences in determining which names to apply for.

8.   Donuts also believes that consumer choice and innovation in the name space

depend significantly on freedom of expression. Donuts forthrightly voices that philosophy in its

response to question 18(a) of all its applications, as follows:

> This TLD is attractive and useful to end-users as it better facilitates
>
> search, self-expression, information sharing and the provision of
>
> legitimate goods and services. Along with the other TLDs in the Donuts
>
> family, this TLD will provide Internet users with opportunities for online
>
> identities and expression that do not currently exist. In doing so, the TLD
>
> will introduce significant consumer choice and competition to the Internet
>
> namespace – the very purpose of ICANN's new TLD program.
>
> This TLD is a generic term and its second level names will be
>
> attractive to a variety of Internet users. Making this TLD available to a
>
> broad audience of registrants is consistent with the competition goals of
>
> the New TLD expansion program, and consistent with ICANN's objective
>
> of maximizing Internet participation. Donuts believes in an open Internet
>
> and, accordingly, we will encourage inclusiveness in the registration
>
> policies for this TLD. In order to avoid harm to legitimate registrants,
>
> Donuts will not artificially deny access, on the basis of identity alone

(without legal cause), to a TLD that represents a generic form of activity

and expression.

9.   From participating in the development of the new gTLD program, Donuts also

understands that the significant expansion resulting from it raised concerns among stakeholders

for preserving the rights of others and protecting users from misconduct. These concerns led

Donuts to support and ICANN to oblige new gTLD applicants to take 14 additional actions that

existing gTLDs do not. Applicant enumerates and commits to implementing each such

requirement in response to question 18(a) of all its applications.

10.   Such new measures are designed to maximize the ability of the registry to

address issues quickly and effectively if and when they arise. Consistent with the objectives of

the program, the new requirements do not seek to prevent potential problems by denying

access to users. Donuts agrees with this approach as well, stating in its applications:

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

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

1. Periodic audit of Whois data for accuracy;

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

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

4. A new Claims Plus product for trademark protection;

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

6. Limitations on domain proxy and privacy service;

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

8. Proper resourcing for all of the functions above.

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

- Whois audits and takedown procedures allow for verification of registrant identity and the right to take action against fraudulent registrant.

- Terms of use and published policies also permit Donuts to act in situations where existing registries either refuse or have no right to do so.

- Donuts' DPML and Claims Plus process, combined with the ICANN-required safeguards, including the Uniform Rapid Suspension (URS) process (the initial recommendation of which I co-authored) offer unprecedented protections to trademark owners that will help them police and take action against misuse of their marks online.

- The "resourcing" Donuts will provide to implement these measures includes a compliance staff dedicated full-time to address such issues.

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

12.   Further, as to this Domain and others deemed potentially sensitive, Donuts has taken four additional steps to shield users from potential misconduct. These include: (i) more frequent and extensive Whois data verification and enhanced take-down processes; (ii) exclusion of registrars with poor compliance history; (iii) regular affirmative registry monitoring for fraud and other forms of misconduct; and (iv) requiring elevated security measures by registrars.

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

14.   Finally, Donuts has passed ICANN's background screening process for over 30 of its 307 applications to date. (ICANN is screening its more than 1,900 applications in an order established by a random drawing that took place several months ago.) Thus, ICANN has determined that Donuts is amply fit to operate a registry.

Donuts' Investment

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

16.   With the ICANN fee of $185,000 per application, Donuts has invested nearly $57 million simply to file its new gTLD applications. It has invested millions more for technical and other support to operate the registries for those gTLDs if and when issued them. It has not done so lightly or with anything less than the highest standards for dependable operation, open access and effective security. Not meeting its own expectations would not merely compromise

its ideals; such failure would also harm its business. Donuts has not raised well over a hundred million dollars to do a poor job and lose its investors' considerable capital.
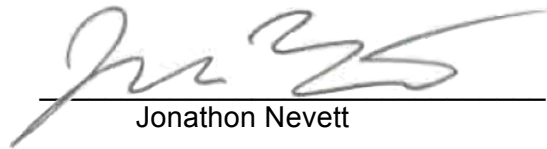
<div align="center"><u>*Matters Raised by the Instant Objection*</u></div>

17.   In response to the Objection's accusations that the Domain may somehow harm the hospital "community" alleged by Objector, I note that Donuts has sought to determine the extent to which the word comprising the Domain at issue here appears at the second level in six existing TLDs – <.com>, <.org>, <.net>, <.info>, <.biz> and <.us>. I directed this survey and know how it was done. Each of these registries must publish a "zone file," listing each of the second level domain names contained in each registry (e.g., there are in excess of 110 million second level names in <.com>). By analyzing these "zone files", we uncovered 26,074 uses of the term "hospital" at the second level of the six investigated TLDs.

18.   Concerned with the volume of objections brought against Donuts by the IO, I have had some research done concerning his background and, in particular, connections to hospital-related concerns. It appears from his *curriculum vitae*, accessible on his website and an accurate copy of which is attached hereto as Exhibit 3, that Professor Pellet has worked with the World Health Organization (WHO). The research also identified a LinkedIn connection between Professor Pellet's legal assistant, Julien Boissise, and Rosa Delgado, a consultant to WHO. *See* http://www.linkedin.com/pub/julien-boissise/5a/b43/197, http://www.linkedin.com/pub/rosa-m-delgado/0/304/24. I understand that Ms. Delgado actively advocated on behalf of the International Medical Informatics Association (IMIA) in proceedings involving the ICANN At-Large Advisory Committee (ALAC). A true and correct copy from the Internet of an exchange involving her and a <.health> community objection is attached hereto as Exhibit 4. ALAC since has brought a community objection on IMIA's behalf against Donuts' <.health> gTLD application, ICC Case No. EXP/505/ICANN/122. I further understand that Ms. Delgado has blogged her views regarding health-related new gTLDs, and attach as Exhibit 5 a true and correct copy of a blog post of hers on the subject. I make these points not to suggest that Professor Pellet has done anything improper, but merely to emphasize his proclivity toward

health-related issues as a possible explanation for his attention during this process to Donuts and its new gTLD applications pertaining to the subject.

I declare under penalty of perjury under the laws of the United States that based on my knowledge and belief the foregoing is true and correct and that this declaration was executed by me on May 15, 2013, in Rockville, Maryland, USA.

_____
Jonathon Nevett

Exhibit 1

[<.hospital> New gTLD Application by Ruby Pike, LLC]

New gTLD Application Submitted to ICANN by: Ruby Pike, LLC

String: hospital

Originally Posted: 13 June 2012

Application ID: 1-1505-15195

Applicant Information

1. Full legal name

```
Ruby Pike, LLC
```

2. Address of the principal place of business

```
155 108th Avenue NE, Suite 510
Bellevue  98004
US
```

3. Phone number
Contact Information Redacted

4. Fax number
Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Daniel Schindler

6(b). Title

EVP, Donuts Inc.

6(c). Address

6(d). Phone Number
Contact Information Redacted

6(e). Fax Number

6(f). Email Address
Contact Information Redacted

Secondary Contact

7(a). Name

Jonathon Nevett

7(b). Title

```
EVP, Donuts Inc.
```

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

```
Limited Liability Company
```

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

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

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

```
Attachments are not displayed on this form.
```

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

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

Dozen Donuts, LLC

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

Applicant Background

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

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

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

| Dozen Donuts, LLC | N∕A |

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

| Paul Stahura | CEO, Donuts Inc |

Applied-for gTLD string

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

hospital

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

16. Describe the applicant's efforts to ensure that there are no known

operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

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

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

Compliance and Interoperability

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

Mixing Scripts

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

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

Interaction Between Labels

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

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

Immature Scripts

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

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

Other Issues

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

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

and relevant language communities to mitigate such issues.

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

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

Mission/Purpose

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

Q18A SV CHAR: 7734

ABOUT DONUTS
Donuts Inc. is the parent applicant for this and multiple other TLDs. The company
intends to increase competition and consumer choice at the top level. It will operate
these carefully selected TLDs safely and securely in a shared resources business
model. To achieve its objectives, Donuts has recruited seasoned executive management
with proven track records of excellence in the industry. In addition to this business
and operational experience, the Donuts team also has contributed broadly to industry
policymaking and regulation, successfully launched TLDs, built industry-leading
companies from the ground up, and brought innovation, value and choice to the domain
name marketplace.

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

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

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

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

The .HOSPITAL TLD will be attractive to registrants with a connection to hospitals and

medical treatment centers around the world. This is a broad and diverse group, and could include health care institutions, teaching hospitals, universities, charitable organizations, medical practitioners, administrators, insurance providers, animal hospitals, and others. The TLD could usefully serve as a place for hospital support efforts, including fundraising and donation; it also can provide a forum for expression regarding hospitals and medical treatment. This widely inclusive TLD would be operated in a secure and legitimate manner.

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

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

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

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

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

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

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

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

13. Implementation DNSSEC; and
14. Measures for the prevention of orphan glue records.

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

1.   For this string, to supplement the periodic audit documented above, a deeper
and more extensive verification of Whois data accuracy, with associated remediation and
takedown processes.
2.   Exclusion of registrars with a history of poor compliance;
3.   Regular monitoring by the registry of registered domains for pharming,
phishing, spam, botnets, copyright infringement and other forms of abuse, and
remediation and takedown processes; and
4.   In addition to registry-based procedures, requirements that registrars have a
24∕7∕365 abuse contact, and remediation and takedown processes.

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

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

Q18B SV CHAR: 8719

DONUTS' PLACE WITHIN ICANN'S MISSION

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

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

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

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

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

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

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

THE GOAL OF THIS TLD

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

SERVICE LEVELS

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

REPUTATION

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

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

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

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

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

NAMESPACE COMPETITION

This TLD will contribute significantly to the current namespace. It will present multiple new domain name alternatives compared to existing generic and country code TLDs. The DNS today offers very limited addressing choices, especially for registrants who seek a specific identity.

INNOVATION

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

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

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

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

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

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

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

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

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

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

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

costs?

Q18C Standard CHAR: 1440

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

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

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

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

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

Q22 CHAR: 4979

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

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

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

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

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

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

2. The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World.

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

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

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

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

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

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

Registry Services

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

Q23 CHAR: 22971

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

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

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

1.0. EXECUTIVE SUMMARY

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

2.0. REGISTRY SERVICES

2.1. Receipt of Data from registrars

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

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

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

to create and manage registrations.

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

2.1.1. SRS EPP Interface

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

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

2.1.1.1. SRS EPP Interface Security Considerations

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

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

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

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

2.1.1.2. SRS EPP Interface Stability Considerations

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

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

2.1.2. SRS Web Interface

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

time as well as the status of the registry services. In addition, notifications that are sent out in email are available for viewing.

2.1.2.1. Web Interface Security Considerations

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

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

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

2.1.2.2. Web Interface Stability Considerations

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

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

2.2. Dissemination of TLD Zone Files

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

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

Normal operations are:

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

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

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

2.2.2. Communication Policy

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

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

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

accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication.

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

2.2.3. Security and Stability Considerations

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

2.3. Zone File Access Provider Integration

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

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

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

2.4. Zone File Update

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

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

2.5. Operation of Zone Servers

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

2.5.1. Security and Operational Considerations of Zone Server Operations

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

The DNS servers are geographically dispersed across multiple secure data centers in

strategic locations around the world. By combining multi-homed servers and geographic diversity, ARI's zone servers remain impervious to site level, supplier level or geographic level operational disruption.

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

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

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

2.6. Dissemination of Domain Registration Information

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

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

2.6.1. Whois Port 43 Interface

The Whois port 43 interface consists of a standard Transmission Control Protocol (TCP) server that answers requests for information over port 43 in compliance with IETF RFC 3912. For each query, the TCP server accepts the connection over port 43 and then waits for a set time for the query to be sent. This communication occurs via clear, unencrypted ASCII text. If a properly formatted and valid query is received, the registry database is queried for the registration data. If registration data exists, it is returned to the service where it is then formatted and delivered to the requesting client. Each query connection is short-lived. Once the output is transmitted, the server closes the connection.

2.6.2. Whois Web Interface

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

2.6.3. Security and Stability Considerations

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

2.7. Internationalized Domain Names (IDNs)

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

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

2.7.1. IDN Stability Considerations

To avoid the intentional or accidental registration of visually similar characters, and
to avoid identity confusion between domains, there are several restrictions on the
registration of IDNs.
Domains registered within a particular language are restricted to only the characters
of that language. This avoids the use of visually similar characters within one
language which mimic the appearance of a label within another language, regardless of
whether that label is already within the DNS or not.
Child domains are restricted to a specific language and registrations are prevented in
one language being confused with a registration in another language; for example
Cyrillic a (U+0430) and Latin a (U+0061).

2.8. DNSSEC

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

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

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

2.8.1. Stability and Operational Considerations for DNSSEC

2.8.1.1. DNSSEC Practice Statement

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

2.8.1.2. Resolution Stability

DNSSEC is considered to have made the DNS more trustworthy; however some transitional

considerations need to be taken into account. DNSSEC increases the size and complexity
of DNS responses. ARI ensures the TLD zone servers are accessible and offer consistent
responses over UDP and TCP.

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

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

3.0. APPROACH TO SECURITY AND STABILITY

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

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

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

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24 CHAR: 19964

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

1.0. INTRODUCTION

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

We will adhere to these commitments by operating a robust and reliable SRS founded on

best practices and experience in the domain name industry.

2.0. TECHNICAL OVERVIEW

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

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

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

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

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

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

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

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

4.0. SOFTWARE QUALITY

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

it. Any failures are automatically assigned to developers to resolve in the morning when they arrive.

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

5.0. SOFTWARE COMPLIANCE

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

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

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

6.0. DATABASE OPERATIONS

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

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

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

7.0. REDUNDANT HARDWARE

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

8.0. HORIZONTALLY SCALABLE

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

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

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

9.0. REDUNDANT HOT FAILOVER SITE

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

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

10.0. SECURE ACCESS

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

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

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

11.0. OPERATING A ROBUST AND RELIABLE SRS

11.1. AUTOMATED DEPLOYMENT

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

11.2. CHANGE MANAGEMENT

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

11.3. PATCH MANAGEMENT

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

11.4. REGULAR BACKUPS

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

11.5. DATA ESCROW

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

11.6. REGULAR TRAINING

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

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

11.7. ACCESS CONTROL

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

11.8. 24∕7 MONITORING AND REGISTRAR TECHNICAL SUPPORT

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

12.0. SRS INFRASTRUCTURE

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

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

13.0 RESOURCING PLAN

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

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

Software Engineering:

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

Systems Engineering:

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

Network Engineering:

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

Database Operations:

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

Information Security Team:

- Existing Department Personnel: Director of Information Security, Sr. Information
Security Specialist, Information Security Specialists, Sr. Information Security
Engineer, Information Security Engineer

- First Year New Hires: Information Security Engineer

Network Operations Center (NOC):

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

25. Extensible Provisioning Protocol (EPP)

Q25 CHAR: 20820

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

1.0. INTRODUCTION

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

2.0. IMPLEMENTATION EXPERIENCE

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

3.0. TRANSPORT

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

4.0. REGISTRARS' EXPERIENCE

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

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

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

Once a registrar has completed testing and is prepared to go live, the registrar is
provided a Scripted Server Environment. This environment contains an EPP interface and

database pre-populated with known data. To verify that the registrar's implementations are correct and minimally suitable for the production environment, the registrar is required to run through a series of exercises. Only after successful performance of these exercises is a registrar allowed access to production services.

5.0. SESSIONS

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

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

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

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

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

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

6.0. EPP SERVICE SCALE

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

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

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

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

7.0. COMPLIANCE WITH CORE AND EPP EXTENSION RFCs

The EPP interface is highly compliant with the following RFCs:

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

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

7.1. RFC 5730 EXTENSIBLE PROVISIONING PROTOCOL

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

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

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

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

Section 2.9 Protocol Commands – compliant

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

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

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

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

7.2. RFC 5731 EPP DOMAIN NAME MAPPING

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

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

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

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

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

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

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

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

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

7.3. RFC 5732 EPP HOST MAPPING

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

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

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

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

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

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

Section 3.2.2 EPP 〈update〉 Command – compliant

Any request to change host name of an external host that has associations with objects
that are sponsored by a different client fails.

7.4. RFC 5733 EPP CONTACT MAPPING

Section 2.1 Contact and Client Identifiers – compliant
Contact identifiers conform to "clIDType" syntax described in RFC 5730.

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

Section 3.1.1 EPP ⟨check⟩ Command – compliant
Maximum of 5 contact id can be checked in a single command request.

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

Section 3.2.2 EPP ⟨delete⟩ Command – compliant
A delete is permitted only if the contact object is not associated with other known
objects.

7.5. RFC 5734 EPP TRANSPORT OVER TCP

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

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

Section 8 Security considerations – ack.
TLS 1.0 over TCP is used to establish secure communications from IP restricted clients.
Validation of authentication credentials along with the certificate common name,
validation of revocation status and the validation of the full certificate chain are
performed. The ACL only allows connections from subnets prearranged with the Registrar.

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

8.0. EPP EXTENSIONS

8.1. STANDARDIZED EXTENSIONS

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

8.2. COMPLIANCE WITH RFC 3735

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

8.3. COMPLIANCE WITH DOMAIN REGISTRY GRACE PERIOD MAPPING RFC 3915

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

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

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

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

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

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

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

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

Section 4.1 DS Data Interface – compliant
The client can provide key data associated with the DS information. The collected key
data along with DS data is returned in an info response, but may not be used in our
systems.

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

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

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

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

8.5. PROPRIETARY EXTENSION DOCUMENTATION

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

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

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

9.0. RESOURCING PLAN

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

Software Engineering:

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

Systems Engineering:

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

Network Engineering:

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

Database Operations:

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

Information Security Team:

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

Network Operations Center (NOC):

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

26. Whois

Q26 CHAR: 19908

1.0.   INTRODUCTION

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

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

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

2.0. HIGH-LEVEL WHOIS SYSTEM DESCRIPTION

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

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

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

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

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

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

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

2.1. PII POLICY

The services and systems for this gTLD do not collect, process or store any personally identifiable information (PII) as defined by state disclosure and privacy laws. Registry systems collect the following Whois data types: first name, last name, address

and phone numbers of all billing, administration and technical contacts. Any business conducted where confidential PII consisting of customer payment information is collected uses systems that are completely separate from registry systems and segregated at the network layer.

3.0. RELEVANT NETWORK DIAGRAM(S)

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

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

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

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

4.0. INTERCONNECTIVITY WITH OTHER REGISTRY SYSTEMS

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

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

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

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

5.0. FREQUENCY OF SYNCHRONIZATION BETWEEN SERVERS

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

6.0. POTENTIAL FORMS OF ABUSE

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

6.1. DATA MINING ABUSE

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

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

6.2. INVALID DATA INJECTION

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

6.3. DISCLOSURE OF PRIVATE INFORMATION

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

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

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

7.1. COMPLIANCE WITH SPECIFICATION 4

Compliance of Whois specifications with Specification 4 is as follows:

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

Evidence of Whois system compliance with this specification consists of:

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

7.2. COMPLIANCE WITH SPECIFICATION 10 FOR WHOIS

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

7.2.1. Emergency Thresholds

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

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

7.2.2. Emergency Escalation

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

8.0. COMPLIANCE WITH RFC 3912

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

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

9.0. RESOURCING PLAN

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

Software Engineering:

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

Systems Engineering:

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

Network Engineering:

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

Database Operations:

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

Information Security Team:

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

Network Operations Center (NOC):

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

11.0. PROVISION FOR SEARCHABLE WHOIS CAPABILITIES

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

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

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

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

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

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

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

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

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

To ensure secure access, a two-factor authentication device is issued to each
authorized user of the registry. Subsequent access to the system requires the user

name, password and a one-time generated password from the issued two-factor device.

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

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

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

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

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

27. Registration Life Cycle

Q27 CHAR: 19951

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

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

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

The registration lifecycle for our gTLD follows core EPP RFCs including RFC 5730 and

RFC 5731 and associated documentation of lifecycle information. To protect registrants, EPP Grace Period Mapping for domain registrations is implemented, which affects the registration lifecycle and domain status. EPP Grace Period Mapping is documented in RFC 3915.

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

4.0. AVAILABILITY
The lifecycle for any domain registration begins with the Available state. This is not necessarily a registration state, per se, but indicates the lack of domain registration implied and provides an entry and terminal point for the state diagram provided. In addition to the state diagram, please refer to Fig. 2 – Availability Check for visual representation of the process flow.

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

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

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

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

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

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

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

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

7.0. REGISTERED STATE

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

8.0. REGISTRATION PERIOD EXTENSION

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

8.1. EXTENSION VIA RENEW REQUEST

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

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

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

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

8.2. EXTENSION VIA TRANSFER PROCESS

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

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

8.3. EXTENSION VIA AUTO-RENEW

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

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

To passively accept the renewal, the registrar need only allow the 45-day time span to

pass for the registration to move out of the Auto Renew Grace Period.

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

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

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

9.0. REQUEST TRANSFER

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

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

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

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

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

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

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

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

successful completion of the transfer process, this status is removed.

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

10.0. REDEMPTION GRACE PERIOD

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

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

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

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

11.0. DELETE

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

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

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

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

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

12.0. ADDITIONAL STATUSES

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

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

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

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

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

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

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

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

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

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

28. Abuse Prevention and Mitigation

Q28 SV CHAR: 30317

1.0. INTRODUCTION

Donuts will employ strong policies and procedures to prevent and mitigate abuse. Our

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

Our approach to abuse prevention and mitigation includes the following:

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

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

2.0. ANTI-ABUSE POLICY

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

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

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

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

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

3.0. TLD ANTI-ABUSE POLICY

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

(1) to protect the integrity and stability of the registry;
(2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
(3) to avoid any liability, civil or criminal, on the part of the registry operator, its affiliates, subsidiaries, officers, directors, or employees;
(4) to comply with the terms of the registration agreement and the registry's Anti-Abuse Policy;
(5) registrant fails to keep Whois information accurate and up-to-date;
(6) domain name use violates the registry's acceptable use policies, or a third party's

rights or acceptable use policies, including but not limited to the infringement of any
copyright or trademark;
(7) to correct mistakes made by the registry operator or any registrar in connection
with a domain name registration; or
(8) as needed during resolution of a dispute.

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

- Distribution of malware: The dissemination of software designed to infiltrate or
damage a computer system without the owner′s informed consent. Examples include
computer viruses, worms, keyloggers, trojans, and fake antivirus products;
- Phishing: attempts to acquire sensitive information such as usernames, passwords, and
credit card details by masquerading as a trustworthy entity in an electronic
communication;
- DNS hijacking or poisoning;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. This
includes but is not limited to email spam, instant messaging spam, mobile messaging
spam, and the spamming of Internet forums;
- Use of botnets, including malicious fast-flux hosting;
- Denial-of-service attacks;
- Child pornography∕child sexual abuse images;
- The promotion, encouragement, sale, or distribution of prescription medication
without a valid prescription in violation of applicable law; and
- Illegal access of computers or networks.

4.0. SINGLE ABUSE POINT OF CONTACT

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

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

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

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

5.0. ABUSE INVESTIGATION AND MITIGATION

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

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

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

Some of these parties typically provide good forensic data or supporting evidence of

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

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

6.0. POLICIES, PROCEDURES, AND SERVICE LEVELS

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

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

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

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

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

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

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

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

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

and allows the registrar to suspend or cancel a domain name.

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

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

7.0. ABUSE MONITORING AND METRICS

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

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

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

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

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

8.0. HANDLING REPORTS FROM LAW ENFORCEMENT, COURT ORDERS

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

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

9.0. PROHIBITING DOMAIN HIJACKINGS AND UNAPPROVED UPDATES

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

10.0. ABUSE POLICY: ADDRESSING INTELLECTUAL PROPERTY INFRINGEMENT

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

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

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

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

11.0. PROPOSED MEASURES FOR REMOVAL OF ORPHAN GLUE RECORDS

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

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

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

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

12.0. METHODS TO PROMOTE WHOIS ACCURACY

12.1. ENFORCING REQUIRED CONTACT DATA FIELDS

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

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

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

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

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

12.2. POLICIES AND PROCEDURES TO ENHANCE WHOIS ACCURACY COMPLIANCE

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

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

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

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

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

All accredited registrars have agreed with ICANN to obtain contact information from registrants, and to take reasonable steps to investigate and correct any reported inaccuracies in contact information for domain names registered through them. As part of our RRA (Registry-Registrar Agreement), we will include a policy that allows us to de-accredit any registrar who a) does not respond to our Whois accuracy requests, or b)

fails to update Whois data or delete the name within 15 days of our report of invalid WHOIS data. In order to allow for inadvertent and unintentional mistakes by a registrar, this policy may include a "three strikes" rule under which a registrar may be de-accredited after three failures to comply.

12.3. PROXY∕PRIVACY SERVICE POLICY TO CURB ABUSE

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

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

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

a. Registrants must provide complete and accurate contact information to their registrar (or reseller, if applicable).. Domains that do not meet this policy may be suspended.
b. Registrars and resellers must provide the underlying registrant information to the registry operator, upon written request, during an abuse investigation. This information will be held in confidence by the registry operator.
c. The registrar or reseller must publish the underlying registrant information in the Whois if it is determined by the registry operator or the registrar that the registrant has breached any terms of service, such as the TLD Anti-Abuse Policy.

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

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

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

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

14.0. CONTROLS TO ENSURE PROPER ACCESS TO DOMAIN FUNCTIONS

Our registry incorporates several measures to ensure proper access to domain functions,

including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

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

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

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

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

15.0   ADDITIONAL PROTECTIONS

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

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

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

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

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

16.0. RESOURCING PLAN

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

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

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

29. Rights Protection Mechanisms

Q29 SV CHAR: 25795

1.0. INTRODUCTION

To minimize abusive registrations and other activities that affect the legal rights of
others, our approach includes well-developed policies for rights protection, both
during our TLD's rollout period and on an ongoing basis. As per gTLD Registry Agreement
Specification 7, we will offer a Sunrise Period and a Trademark Claims service during
the required time periods, we will use the Trademark Clearinghouse, and we will
implement Uniform Rapid Suspension (URS) on an ongoing basis. In addition to these
newly mandated ICANN protections, we will implement two other trademark protections
that were developed specifically for the new TLD program. These additional protections
are: (i) a Domain Protected Marks List (DPML) for the blocking of trademarked strings
across multiple TLDs; and (ii) a Claims Plus product to alert registrars to
registrations that potentially infringe existing marks.

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

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

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

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

2.0. NARRATIVE FOR Q29 FIGURE 1 OF 1

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

3.0. PRE-SUNRISE: RESERVED AND PREMIUM NAMES

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

We also will designate certain domains as "premium" domains. These will include domains

based on generic words and one-character domains. These domains will not be available in Sunrise, and the registry may offer them via special means such as auctions and RFPs.

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

4.0. SUNRISE

4.1. SUNRISE OVERVIEW

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

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

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

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

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

4.2. SUNRISE: ELIGIBLE RIGHTS

Our Sunrise Eligibility Requirements (SERs) are:

1. Ownership of a qualifying mark.

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

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

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

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

4.3. SUNRISE TRADEMARK VALIDATION

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

Accordingly, we will validate applications via the Trademark Clearinghouse. We will compare applications to the Trademark Clearinghouse database, and those that match (as

per the Sunrise rules) will be considered valid applications.

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

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

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

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

4.5. CONTENDING APPLICATIONS, SUNRISE AUCTIONS

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

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

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

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

4.6. SUNRISE DISPUTE RESOLUTION PROCESS (SUNRISE CHALLENGES)

We will retain the services of a well-known dispute resolution provider (such as WIPO) to help formulate the language of our Sunrise Dispute Resolution Process (SDRP, or "Sunrise Challenge") and hear the challenges filed under it. All applicants and registrars will be contractually obligated to follow the decisions handed down by the dispute resolution provider.

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

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

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

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

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

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

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

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

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

5.0. TRADEMARK CLAIMS SERVICES

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

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

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

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

"Identical Match" is defined in ICANN's Module 4, "Trademark Clearinghouse" document, paragraph 6.1.5. We will examine the Clearinghouse specifications and protocol

carefully when they are published. To comply with ICANN policy, the software for our registry will properly check domains and compare them to marks in the Clearinghouse that contain punctuation, spaces, and special symbols.

6.0. GENERAL REGISTRATION

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

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

7.0. UNIFORM RAPID SUSPENSION (URS)

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

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

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

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

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

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

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

8.0. ONGOING RIGHTS PROTECTION MECHANISMS - UDRP

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

9.0 ADDITIONAL RIGHTS PROTECTION MECHANISMS NOT REQUIRED BY ICANN

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

ICANN. These new protections are:

9.1   Claims Plus: This service will become available at the conclusion of the Trademark Claims service, and will remain available for at least the first five years of registry operations. Trademark owners who are fully registered in the Trademark Clearinghouse may obtain Claims Plus for their marks. We expect the service will be at low or no cost to trademark owners (contingent on Trademark Clearinghouse costs to registries). Claims Plus operates much like Trademark Claims with the exception that notices of potential trademark infringement are sent by the registry to any registrar whose customer performs a check-command or Whois query for a string subject to Claims Plus. Registrars may then take further implementation steps to advise their customers, or use this data to better improve the customer experience. In addition, the Whois at the registry website will output a full Trademark Claims notice for any query of an unregistered name that is subject to Claims Plus.   (Note: The ongoing availability of Claims Plus will be contingent on continued access to a Trademark Clearinghouse. The technical viability of some Claims Plus features will be affected by eventual Trademark Clearinghouse rules on database caching).

9.2   Domain Protected Marks List: The DPML is a rights protection mechanism to assist trademark holders in protecting their intellectual property against undesired registrations of strings containing their marks. The DPML prevents (blocks) registration of second level domains that contain a trademarked term (note: the standard for DPML is "contains"— the protected string must contain the trademarked term).   DPML requests will be validated against the Trademark Clearinghouse and the process will be similar to registering a domain name so the process will not be onerous to trademark holders. An SLD subject to DPML will be protected at the second level across all Donuts TLDs (i.e. all TLDs for which this SLD is available for registration). Donuts may cooperate with other registries to extend DPML to TLDs that are not operated by Donuts. The cost of DPML to trademark owners is expected to be significantly less than the cost of actually registering a name.

10.0 ABUSIVE USE POLICIES AND TAKEDOWN PROCEDURES

In our response to Question #28, we describe our anti-abuse program, which is designed to address malware, phishing, spam, and other forms of abuse that may harm Internet users. This program is designed to actively discover, verify, and mitigate problems without infringing upon the rights of legitimate registrants. This program is designed for use in the open registration period. These procedures include the reporting of compromised websites∕domains to registrars for cleanup by the registrants and their hosting providers. It also describes takedown procedures, and the timeframes and circumstances that apply for suspending domain names used improperly. Please see the response to Question #28 for full details.

We will institute a contractual obligation that proxy protection be stripped away if a domain is proven to be used for malicious purposes. For details, please see "Proxy∕ Privacy Service Policy to Curb Abuse" in the response to Question 28.

11.0. REGISTRY-REGISTRAR CODE OF CONDUCT AS RELATED TO RIGHTS PROTECTION

We will comply fully with the Registry Code of Conduct specified in the New TLD Registry Agreement, Specification 9.   In rights protection matters, we will comply by establishing an adequate "firewall" between the operations of any registrar we establish and the operations of the registry. As the Code requires, we will not "directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services". Here is a non-exhaustive list of specific steps we will take to accomplish this:

- We will evaluate and execute upon all rights protection tasks impartially, using the same criteria and procedures, regardless of a domain's sponsoring registrar.
- Any registrar we establish or have established at the time of registry launch will not receive preferential access to any premium names, any auctions, etc. Registry personnel and any registrar personnel that we may employ in the future will be prohibited from participating as bidders in any auctions for Landrush names.
- Any registrar staff we may employ in the future will have access to data and records

relating only to the applications and registrations made by any registrar we establish, and will not have special access to data related to the applications and registrations made by other registrars.
- If a compliance function is involved, the compliance staffer will be responsible to the registry only, and not to a registrar we own or are "affiliated" with. For example, if a compliance staff member is assigned to conduct audits of WHOIS data, that staffer will not have duties with the registrar business. The staffer will be free of conflicts of interest, and will be enabled to discharge his or her duties to the registry effectively and impartially, regardless of the consequences to the registrar.

12.0   ADDITIONAL PROTECTIONS

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

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

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

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

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

13.0. RESOURCING PLAN

Overall management of RPMs is the responsibility of Donuts' VP of Business Operations. Our back-end registry operator will perform the majority of operational work associated with RPMs, as required by our agreement with them. Donuts VP of Business Operations will supervise the activity of this vendor.

Resources applied to RPMs include:

1. Legal team
a. We will have at least one legal counsel who will be dedicated to the registry with previous experience in domain disputes and Sunrise periods and will oversee the compliance and support teams with regard to the legal issues related to Sunrise and RPM's
b. We have outside counsel with domain and rights protection experience that is available to us as necessary
2. Dispute Resolution Provider (DRP): The DRP will help formulate Sunrise Rules and Policy, Sunrise Dispute Resolution Policy. The DRP will also examine challenges, but the challenger will be required to pay DRP fees directly to the DRP.
3. Compliance Department and Tech Support: There will be three dedicated personnel assigned to these areas. This staff will oversee URS requests and abuse reports on an ongoing basis.
4. Programming and technical operations. There are four dedicated personnel assigned to these functions.
5. Project Manager: There will be one person to coordinate the technical needs of this group with the registry IT department.

13.0. ENDNOTES

1 "Regional" is understood to be a trans-national trademark registry, such as the European Union registry or the Benelux Office for Intellectual Property.

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

registry

Q30a SV Char: 19960

1.0   INTRODUCTION

Our Information Security (IS) Program and associated IS Policy, Standards and
Procedures apply to all Applicant entities, employees, contractors, temps, systems,
data, and processes. The Security Program is managed and maintained by the IS Team,
supported by Executive Management and the Board of Directors.

Data and systems vary in sensitivity and criticality and do not unilaterally require
the same control requirements. Our security policy classifies data and systems types
and their applicable control requirements. All registry systems have the same data
classification and are all managed to common security control framework. The data
classification applied to all registry systems is our highest classification for
confidentiality, availability and integrity, and the supporting control framework is
consistent with the technical and operational requirements of a registry, and any
supporting gTLD string, regardless of its nature or size. We have the experienced
staff, robust system architecture and managed security controls to operate a registry
and TLD of any size while providing reasonable assurance over the security,
availability, and confidentiality of the systems supporting critical registry functions
(i.e., registration services, registry databases, zone administration, and provision of
domain name resolution services).

This document describes the governance of our IS Program and the control frameworks our
security program aligns to (section 1.0), Security Policy requirements (section 2.0);
security assessments conducted (see section 3.0), our process for executive oversight
and visibility of risks to ensure continuous improvement (section 4.0), and security
commitments to registrants (section 5). Details regarding how these control
requirements are implemented, security roles and responsibilities and resources
supporting these efforts are included in Security Policy B response.

2.0. INFORMATION SECURITY PROGRAM

The IS Program for our registry is governed by an IS Policy aligned to the general
clauses of ISO 27001 requirements for an Information Security Management System (ISMS)
and follows the control objectives where appropriate, given the data type and resulting
security requirements. (ISO 27001 certification for the registry is not planned,
however, our DNS∕DNSSEC solution is 27001 certified). The IS Program follows a Plan-Do-
Check-Act (PDCA) model of continuous improvement to ensure that the security program
grows in maturity and that we provide reasonable assurance to our shareholders and
Board of Directors that our systems and data are secure.

The High Security Top Level Domain (HSTLD) control framework incorporates ISO 27002,
the code of practice for implementing an ISO 27001 ISMS. Therefore, our security
program is already closely aligned to the HSTLD control framework. Furthermore, we
agree to abide by the HSTLD Principle 1 and criteria 1.1 - 1.3. (See specifics in
Security Policy B response):

Registry systems will be in-scope for Sarbanes-Oxley (SOX) compliance and will follow
the SOX control framework governing access control, account management, change
management, software development life cycle (SDLC), and job monitoring of all systems.
Registry systems will be tested frequently by the IS team for compliance and audited by
our internal audit firm, Protiviti, and external audit firm, Price Waterhouse Coopers
(PWC), for compliance.

2.1. SECURITY PROGRAM GOVERNANCE

Our Information Security Program is governed by IS Policy, supported by standards, and
guided by procedures to ensure uniformed compliance to the program. Standards and
associated procedures in support of the policy are shown in Attachment A, Figure 1.
Security Program documents are updated annually or upon any system or environment
change, new legal or regulatory requirements, and∕or findings from risk assessments.

Any updates to security program are reviewed and approved by the Executive Vice
President of IT, the General Counsel, and the EVP of HR before dissemination to all
employees.

All employees are required to sign the IS Policy upon hire, upon any major changes,
and∕or annually. By signing the IS Policy, employees agree to abide by the supporting
Standards and Procedures applicable to their job roles. To enable signing of the IS
Policy, employees must pass a test to ensure competent understanding of the IS Policy
and its key requirements.

3.0. INFORMATION SECURITY POLICY

3.1. INFORMATION ASSET CLASSIFICATION

The following data classification is applied to registry systems: High Business Impact
(HBI): Business Confidential in accordance with the integrity, availability and
confidentiality requirements of registry operations. All registry systems will follow
Security Policy requirements for HBI systems regardless of the nature of the TLD
string, financial materiality or size. HBI data if not properly secured, poses a high
degree of risk to the registry and includes data pertaining to the registry's adherence
to legal, regulatory and compliance requirements, mergers and acquisitions (M&A), and
confidential data inclusive of, but is not limited to: Personally Identifiable
Information (PII) (credit card data, Social Security Numbers (SSN) and account
numbers); materially important financial information (before public disclosure), and
information which the Board of Directors (BoD)∕Executive team deems to be a trade
secret, which, if compromised, would cause grave harm to the execution of our business
model.

HBI safeguards are designed, implemented and measured in alignment with
confidentiality, integrity, availability and privacy requirements characterized by
legal, regulatory and compliance obligations, or through directives issued by the BoD
and Executive team. Where guidance is provided, such as the Payment Card Industry (PCI)
Data Security Standard (DSS) Internal Audit Risk Control Matrices (RCMs), local, state
and federal laws, and other applicable regulations, we put forth the appropriate level
of effort and resources to meet those obligations. Where there is a lack of guidance or
recommended safeguards, Risk Treatment Plans (RTP's) are designed in alignment with our
standard risk management practices.

Other data classifications for Medium Business Impact (MBI): Business Sensitive and Low
Business Impact (LBI): Public do not apply to registry systems.

3.2. INFORMATION ASSET MANAGEMENT

All registry systems have a designated owner and∕or custodian who ensure appropriate
security classifications are implemented and maintained throughout the lifecycle of the
asset and that a periodic review of that classification is conducted. The system owner
is also responsible for approving access and the type of access granted. The IS team,
in conjunction with Legal, is responsible for defining the legal, regulatory and
compliance requirements for registry system and data.

3.3. INFORMATION ASSET HANDLING, STORAGE & DISPOSAL

Media and documents containing HBI data must adhere to their respective legal,
regulatory and compliance requirements and follow the HBI Handling Standard and the
retention requirements within the Document Retention Policy.

3.4. ACCESS CONTROL

User authentication is required to access our network and system resources. We follow a
least-privileged role based access model. Users are only provided access to the
systems, services or information they have specifically been authorized to use by the
system owner based on their job role. Each user is uniquely identified by an ID
associated only with that user. User IDs must be disabled promptly upon a user's
termination, or job role change.

Visitors must sign-in at the front desk of any company office upon arrival and escorted by an employee at all times. Visitors must wear a badge while on-site and return the badge when signing out at the front desk. Dates and times of all visitors as well as the name of the employee escorting them must be tracked for audit purposes.

Individuals permitted to access registry systems and HBI information must follow the HBI Identity & Access Management Standard. Details of our access controls are described in Part B of Question 30 response including; technical specifications of access management through Active Directory, our ticketing system, physical access controls to systems and environmental conditions at the datacenter.

3.5. COMMUNICATIONS & OPERATIONAL SECURITY

3.5.1. MALICIOUS CODE

Controls shall be implemented to protect against malicious code including but not limited to:
- Identification of vulnerabilities and applicable remediation activities, such as patching, operating system & software upgrades and∕or remediation of web application code vulnerabilities.
- File-integrity monitoring shall be used, maintained and updated appropriately.
- An Intrusion Detection Solution (IDS) must be implemented on all HBI systems, maintained & updated continuously.
- Anti-virus (AV) software must be installed on HBI classified web & application systems and systems that provide access to HBI systems. AV software and virus definitions are updated on a regular basis and logs are retained for no less than one year.

3.5.2. THREAT ANALYSIS & VULNERABILITY MANAGEMENT

On a regular basis, IS personnel must review newly identified vulnerability advisories from trusted organizations such as the Center for Internet Security, Microsoft, SANS Institute, SecurityFocus, and the CERT at Carnegie-Mellon University. Exposure to such vulnerabilities must be evaluated in a timely manner and appropriate measures taken to communicate vulnerabilities to the system owners, and remediate as required by the Vulnerability Management Standard. Internal and external network vulnerability scans, application & network layer penetration testing must be performed by qualified internal resource or an external third party at least quarterly or upon any significant network change. Web application vulnerability scanning is to be performed on a continual basis for our primary web properties applicable to their release cycles.

3.5.3. CHANGE CONTROL

Changes to HBI systems including operating system upgrades, computing hardware, networks and applications must follow the Change Control Standard and procedures described in Security Policy question 30b.

3.5.4. BACKUP & RESTORATION

Data critical to our operations shall be backed up according to our Backup and Restoration Standard. Specifics regarding Backup and Restoration requirements for registry systems are included in questions 37 & 38.

3.6. NETWORK CONTROLS

 - Appropriate controls must be established for ensuring the network is operated consistently and as planned over its entire lifecycle.
 - Network systems must be synchronized with an agreed upon time source to ensure that all logs correctly reflect the same accurate time.
 - Networked services will be managed in a manner that ensures connected users or services do not compromise the security of the other applications or services as required in the HBI Network Configuration Standard. Additional details are included in Question 32: Architecture response.

3.7. DISASTER RECOVERY & BUSINESS CONTINUITY

The SVP of IT has responsibility for the management of disaster recovery and business continuity. Redundancy and fault-tolerance shall be built into systems whenever possible to minimize outages caused by hardware failures. Risk assessments shall be completed to identify events that may cause an interruption and the probability that an event may occur. Details regarding our registry continuity plan are included in our Question 39 response.

3.8 SOFTWARE DEVELOPMENT LIFECYCLE

Advance planning and preparation is required to ensure new or modified systems have adequate security, capacity and resources to meet present and future requirements. Criteria for new information systems or upgrades must be established and acceptance testing carried out to ensure that the system performs as expected. Registry systems must follow the HBI Software Development Lifecycle (SDLC) Standard.

3.9. SECURITY MONITORING

Audit logs that record user activities, system errors or faults, exceptions and security events shall be produced and retained according to legal, regulatory, and compliance requirements. Log files must be protected from unauthorized access or manipulation. IS is responsible for monitoring activity and access to HBI systems through regular log reviews.

3.10. INVESTIGATION & INCIDENT MANAGEMENT RESPONSE

Potential security incidents must be immediately reported to the IS Team, EVP of IT, the Legal Department and∕or the Incident Response email alias. The Incident Response Team (IRT) is required to investigate: any real or suspected event that could impact the security of our network or computer systems; impose significant legal liabilities or financial loss, loss of proprietary data∕trade secret, and∕or harm to our goodwill. The Director of IS is responsible for the organization and maintenance of the IRT that provides accelerated problem notification, damage control, investigation and incident response services in the event of security incidents. Investigation and response processes follow the requirements of the Investigation and Incident Management Standard and supporting Incident Response Procedure (see Question 30b for details).

3.11. LEGAL & REGULATORY COMPLIANCE

All relevant legal, regulatory and contractual requirements are defined, documented and maintained within the IS Policy. Critical records are protected from loss, destruction and falsification, in accordance with legal, contractual and business requirements as described in our Document Retention Policy. Compliance programs implemented that are applicable to Registry Services include:

- Sarbanes Oxley (SOX): All employees managing and accessing SOX systems and∕or data are required to follow SOX compliance controls.
- Data Privacy and Disclosure of Personally Identifiable Information (PII): data protection and privacy shall be ensured as required by legal and regulatory requirements, which may include state breach and disclosure laws, US and EU Safe Harbor compliance directives.

Other compliance programs implemented but not applicable to Registry systems include the Payment Card Industry (PCI) Data Security Standard (DSS), Office of Foreign Assets Control (OFAC) requirements, Copyright Infringement & DMCA.

4.0. SECURITY ASSESSMENTS

Our IS team conducts frequent security assessments to analyze threats, vulnerabilities and risks associated with our systems and data. Additionally, we contract with several third parties to conduct independent security posture assessments as described below. Details of these assessments are provided in our Security Policy B response.

4.1. THIRD PARTY SECURITY ASSESSMENTS

We outsource the following third party security assessments (scope, vendor, frequency and remediation requirements of any issues found are detailed in our Security Policy B response); Web Application Security Vulnerability testing, quarterly PCI ASV scans, Sarbanes-Oxley (SOX) control design and operating effectiveness testing and Network and System Security Analysis.

4.2. INTERNAL SECURITY ASSESSMENTS

The IS team conducts routine and continual internal testing (scope, frequency, and remediation requirements of any issues found are detailed in our Security Policy B response) including; web application security vulnerability testing, external and internal vulnerability scanning, system and network infrastructure penetration testing, access control appropriateness reviews, wireless access point discovery, network security device configuration analysis and an annual comprehensive enterprise risk analysis.

5.0. EXECUTIVE OVERSIGHT & CONTINUOUS IMPROVEMENT

In addition to the responsibility for Information Security residing within the IS team and SVP of IT, risk treatment decisions are also the responsibility of the executive of the business unit responsible for the risk. Any risk with potential to impact the business financially or legally in a material way is overseen by the Incident Response Management team and∕or the Audit Committee. See Figure 2 in Attachment A. The Incident Response Management Team or Audit Committee will provide assistance with management action plans and remediation.

5.1. GOVERNANCE RISK & COMPLIANCE

We have deployed RSA's Archer Enterprise Governance Risk and Compliance (eGRC) Tool to provide an independent benchmarking of risk, compliance and security metrics, assist with executive risk reporting and reduce risk treatment decision making time, enforcing continuous improvement. The eGRC provides automated reporting of registry systems compliance with the security program as a whole, SOX Compliance, and our Vulnerability Management Standard. The eGRC dashboard continuously monitors risks and threats (through automated feeds from our vulnerability testing tools and third party data feeds such as Microsoft, CERT, WhiteHat, etc.) that are actionable. See Attachment A for more details on the GRC solutions deployed.

6.0. SECURITY COMMITMENTS TO REGISTRANTS

We operate all registry systems in a highly secured environment with appropriate controls for protecting HBI data and ensuring all systems remain confidential, have integrity, and are highly available. Registrants can assume that:

1. We safeguard the confidentiality, integrity and availability of registrant data through access control and change management:
 - Access to data is restricted to personnel based on job role and requires 2 factors of authentication.
 - All system changes follow SOX-compliant controls and adequate testing is performed to ensure production pushes are stable and secure.
2. The network and systems are deployed in high availability with a redundant hot datacenter to ensure maximum availability.
3. Systems are continually assessed for threats and vulnerabilities and remediated as required by the Vulnerability Management Standard to ensure protection from external malicious acts.
 - We conduct continual testing for web code security vulnerabilities (cross-site scripting, SQL Injection, etc.) during the development cycle and in production.
4. All potential security incidents are investigated and remediated as required by our Incident Investigation & Response Standard, any resulting problems are managed to prevent any recurrence throughout the registry.

We believe the security measures detailed in this application are commensurate with the nature of the TLD string being applied for. This string might be considered by some to have public trust implications (as discussed in Guidebook Q30), accordingly, the following additional security measures will be implemented to protect consumers using

this TLD including, but not limited to:

1.   Periodic audit of Whois data for accuracy.
2.   Deeper and more extensive verification of Whois data accuracy, with associated remediation and takedown processes.
3.   Regular monitoring of registered domains for pharming, phishing, spam, botnets, copyright infringement and other forms of abuse, and remediation and takedown processes.
4.   A new Domain Protected Marks List (DPML) product for trademark protection;
5.   A new Claims Plus product for trademark protection;
6.   Terms of use that prohibit illegal or abusive activity;
7.   Limitations on domain proxy and privacy service;
8.   Published policies and procedures that define abusive activity
9.   Require that registrars have a 24∕7∕365 abuse contact and a remediation ∕ takedown processes.
10.   Exclusion of registrars with a history of poor compliance.
11.   Proper resourcing for all of the functions above.

7.0   RESPONSIBILITY OF INFORMATION SECURITY
See Question B Response Section 10.

Exhibit 2

[List of new gTLDs applied for by Donuts Inc.]

ACADEMY	ACCOUNTANTS	AGENCY
APARTMENTS	APP	ARCHITECT
ART	ASSOCIATES	ATTORNEY
AUCTION	AUDIO	AUTO
BABY	BAND	BARGAINS
BASEBALL	BASKETBALL	BEAUTY
BET	BIKE	BINGO
BLOG	BOATS	BOOK
BOUTIQUE	BROADWAY	BROKER
BUILDERS	BUSINESS	BUY
CAB	CAFÉ	CAMERA
CAMP	CAPITAL	CARDS
CARE	CAREERS	CARS
CASA	CASH	CASINO
CATERING	CENTER	CHARITY
CHAT	CHEAP	CHURCH
CITY	CLAIMS	CLEANING
CLINIC	CLOTHING	CLOUD
CLUB	COACH	CODES
COFFEE	COLLEGE	COMMUNITY
COMPANY	COMPUTER	CONDOS
CONSTRUCTION	CONSULTING	CONTRACTORS
COOL	CORP	COUPONS
CPA	CREDIT	CREDITCARD
CRICKET	CRUISES	DATA
DATING	DEALS	DEGREE
DELIVERY	DENTAL	DENTIST
DESIGN	DIAMONDS	DIET
DIGITAL	DIRECT	DIRECTORY
DISCOUNT	DOCTOR	DOG
DOMAINS	ECO	EDUCATION
EMAIL	ENERGY	ENGINEERING
ENTERPRISES	EQUIPMENT	ESTATE
EVENTS	EXCHANGE	EXPERT
EXPOSED	EXPRESS	FAIL
FAMILY	FAN	FARM
FASHION	FILM	FINANCE
FINANCIAL	FISH	FITNESS
FLIGHTS	FLORIST	FLOWERS

FOOD	FOOTBALL	FORSALE
FORUM	FOUNDATION	FREE
FUND	FURNITURE	FUTBOL
FYI	GALLERY	GAMES
GARDEN	GIFTS	GLASS
GLOBAL	GMBH	GOLD
GOLF	GRAPHICS	GRATIS
GRIPE	GROUP	GUIDE
GURU	HAUS	HEALTH
HEALTHCARE	HELP	HOCKEY
HOLDINGS	HOLIDAY	HOME
HOSPITAL	HOSTING	HOT
HOTEL	HOUSE	IMMO
INC	INDUSTRIES	INSTITUTE
INSURANCE	INSURE	INTERNATIONAL
INVESTMENTS	JEWELRY	JUEGOS
KITCHEN	LAND	LAW
LAWYER	LEASE	LEGAL
LIFE	LIGHTING	LIMITED
LIMO	LIVE	LIVING
LLC	LOANS	LOVE
LTD	LUXURY	MAIL
MAISON	MANAGEMENT	MARKET
MARKETING	MBA	MEDIA
MEDICAL	MEMORIAL	MOBILE
MONEY	MORTGAGE	MOVIE
MUSIC	NETWORK	NEWS
NOW	ONLINE	PARTNERS
PARTS	PETS	PHONE
PHOTOGRAPHY	PHOTOS	PICTURES
PIZZA	PLACE	PLUMBING
PLUS	POKER	PRODUCTIONS
PROPERTIES	PROPERTY	RACING
RADIO	REALESTATE	REALTY
RECIPES	RED	REISEN
RENT	RENTALS	REPAIR
REPORT	RESTAURANT	REVIEWS
ROCKS	RUGBY	RUN
SALE	SALON	SARL
SCHOOL	SCHULE	SEARCH
SECURITY	SERVICES	SHOES
SHOP	SHOPPING	SHOW
SINGLES	SITE	SKI
SOCCER	SOFTWARE	SOLAR
SOLUTIONS	SPA	SPORTS
STORAGE	STORE	STUDIO

STYLE	SUCKS	SUPPLIES
SUPPLY	SUPPORT	SURGERY
SYSTEMS	TAX	TAXI
TEAM	TECH	TECHNOLOGY
TENNIS	THEATER	TICKETS
TIENDA	TIPS	TIRES
TODAY	TOOLS	TOURS
TOWN	TOYS	TRADING
TRAINING	TUBE	UNIVERSITY
VACATIONS	VENTURES	VET
VIAJES	VIDEO	VILLAS
VIN	VIP	VISION
VOTE	VOYAGE	WATCH
WEB	WEBSITE	WEDDING
WINE	WORKS	WORLD
WTF	YOGA	ZONE

游戏　GAMES
商店 SHOP or STORE
娱乐　ENTERTAINMENT
企业　ENTERPRISE

<u>Exhibit 3</u>

[Alain Pellet *curriculum vitae*]

ALAIN PELLET

Professor, University Paris Ouest, Nanterre-La Défense,
Former Member and Former Chairperson, International Law Commission
of the United Nations,
Designated to the Panel of Arbitrators of the ICSID by the Chairman of the Administrative
Council, Associé de l'Institut de Droit international

Contact Information Redacted

Address :   Contact Information Redacted

CURRICULUM VITAE

ACADEMIC QUALIFICATIONS :

-   Agrégation in public law and political science (1974)

-   State Doctorate in public law (1974 - University of Paris II, Panthéon - Assas)

-   Diploma of advanced studies in public law (1969 - Faculty of Law and Economics, Paris)

-   Diploma of advanced studies in political science (1969 - Faculty of Law and Economics, Paris)

-   Diploma of the Institute of Political Studies, Paris (Sciences-Po) (1968 - public service section,)

-   Bachelor of laws (public law) (1968 - Faculty of Law and Economics, Paris)

-   Auditor at the Academy of International Law, The Hague (public international law courses, 1967, 1969 and 1971)

FOREIGN LANGUAGES :

-   English : read, speak, write

-   Italian : read and speak (poorly)

POSTS :

- At the University Paris Ouest, Nanterre-La Défense,

  Professor (1990 -   )

     Courses given :
            - General Public International Law (degree course, third year)
            - International Development Law (Master's degree)
            - Special Public International Law (Master's degree)
            - International Law of the Economics (Post-graduate studies)
            - The International Legal System (Post-graduate studies)

  Director of the Centre for International Law (CEDIN – 1991-2001)

  Director, Post-graduate Studies in International and European Law of Economics Relations (1991-2009), then Co-director (with Jean-Marc Thouvenin) of the Master 2 (research) Laws of International Relations and of the European Union (2009-   ).

  Member of the Faculty Board (1995 - 2003)

  Chairman of the Commission of Specialists in Public Law (1998 - 2007); Member (1990 - 2008); Member of the consultative Committee – Public Law (2009 -   ).

- At the Institute of Political Studies, Paris (Sciences-Po)

  Professor (1980 - 1999)

     Courses given :
          "The legal framework of international relations" (1990 - 1999)
          "The legal framework of international economic life" (1980 - 1989)

  From 1972 to 1975 and from 1977 to 1981, Senior Lecturer in international law (International relations section, second and third years)

  From 1970 to 1975, leader of a seminar on international relations (with Professor M. Merle).

- At the Faculty of Law and Political Science of the University of Paris-Nord :

  Professor (1974 - 1990) (seconded to the University of Constantine until 15 september 1977)

     Courses given :
            - Public international law (general course) (degree course, third year)
            - International development law (degree course, fourth year)
            - International economic law (post-graduate studies in public law and business law)

       - International administrative law (post-graduate studies in public law)

Member of the University Council and the Scientific Council (1979 - 1986)

Director of the Study Group on International law, economics and development (GERDIED)

Delegate for international relations of the University (1978 - 1982)

Vice-Dean (1981 - 1982)

Member of the Faculty Board (1978 - 1982 and 1987 - 1990)

Chairman of the Commission of Specialists in Public Law and Political Science (1985 - 1990)

-     At the University of Constantina (Algeria) :

From 1975 to 1977, Agrégé Professor in public law, seconded by the University of Paris-Nord under the civilian cultural co-operation scheme.

    Courses given :
        - International development law (degree course, fourth year)
        - Petroleum law (degree course, fourth year)
        - Public international law, general course (three semesters, degree course, third and fourth years)

-     At the National School of Administration, Algiers :

From 1975 to 1977, Professor

    Courses given :
        The law of international organizations (diplomatic section)
        General public international law (general section and diplomatic section)

-     Lecturer at the Faculty of Law and Economics, Paris, and at the University of Law, Economics and Social Sciences, Paris, from 1968 to 1974

-     At René Descartes University (Paris V) - Institute of Legal Sciences of Development :

Courses and Seminars in International Law of Development (1978-1988)

-     At the National School of Administration, Paris :

Member of the admissions panel (1980 : second external competitive examination; 1981 : first external competitive examination and of the graduation panel (1982))

Course on the "framing" of international relations : "Third world and development - legal aspects" (1984 - 1985)

-     <u>At the University of Law, Economics and Social Sciences, Paris (IHEI) :</u>

Courses on "International law, disarmament and development" (1979 - 1980) and on "The codification of the law of international responsability" (1994 - 1995)

LECTURES, MISSIONS ABROAD, GUEST PROFESSOR :

Consejo Argentino para las Relaciones Internationales (CARI) (Buenos Aires) (2011)
Universidad de Buenos Aires, Facultad de Derecho (Buenos Aires) (2011)
Yale Law School (2010)
Instituto del Servicio Exterior de la Nación (Buenos Aires) (2010)
Université Laval, Québec (2009)
Diplomatic Academy Bucharest (2006)
Université Lyon III (2005)
University of Singapore (2004 and 2008)
Universidad del Rosario, Bogota (2004)
Universidad Centroamericana, Managua (2004)
University Carlos III, Madrid (2002)
Waseda University, Tokyo (2001)
Humboldt University, Berlin (2000)
University of Helsinki (2000)
State University, Higher School of Economics, Moscow (1999)
Law Faculty, Edinburgh (1999)
Universities of São Paulo (USP), Brasilia (Catholic University, UnB, Instituto Rio Branco), Belo Horizonte (UFMG) and Rio de Janeiro (PUC/RJ, University Estácio de Sá and UERJ) (1998)
University of French West Indies and Guyana, Fort-de-France (1997, 2001, 2006, 2008 and 2009)
Dong-A University (Pusan, South Korea) (1997)
MGIMO (Moscow) (1996)
International Development Law Institute (Rome) (1995)
British Institute of International and Comparative Law (London) (1994, 1998)
Faculty of Law of Sarrebrück (Germany) (1994)
Faculty of Law of Granada (Spain) (1992)
International Institute of Postgraduate Studies (Geneva) (1992, 2007 and 2009)
New York University (1991)
European University Institute, Florence, (1990)
University of Mauricius, School of Law (1989)
Faculty of Law of Athens (1988)
University College (London) (1986)
Faculty of Law of Tunis (1985, 1988, 1992, 1995)
Faculty of Law of Casablanca (Morroco) (1984)
Warwick University (England) (1984)
Faculty of Law of Damascus (Syria) (1983)
Center for External Relations Dar-es-Salaam (Tanzania) (1982)
United Nations University (Tokyo - 1981) (Cairo - 1983)

University Mohamed V of Rabat (Morocco) (1981, 1982)
National University of Benin (1979)
University of French West Indies and Guyana, Pointe-à-Pitre (1979-1986, 1992, 1994-1996, 1999-2006)
Thammasat University of Bangkok (Thaïland) (1978)
University of Constantina (1978, 1979, 1980, 1982)
University of Algiers (1977)

- At the Centre for International Law (CEDIN), Faculty of Law, Federal University of Minas Gerais (Belo Horizonte - Brazil) – Winter Courses

   General Course in Public International law: "International Law between State Sovereignty and the International Community – The Law-Making Process in Public International Law" (2005)

   Course: "International law in its infinite variety – eulogy of the *soft law*" (2009)

- At the *Centro Internacional Bancaja Para la Paz y el Desarollo* (Castellón, Spain) :

   Basic Course: "International Law on the Eve of the XXIst Century - The Law of the International Society" (1997)

- At the International Institute of Human Rights (René Cassin) (Strasbourg) :

   Course : "The International Criminal Responsability of the Individual" (1995)

- At the Academy of European Law (Florence) :

   Course : "The International Legal Foundations of the European Communities Law" (1994)

- At the International Law Institute, Thessalonica :

   Course, "Aspects of the normative process in international economic and development law" (1988)

   Course, "Criminalizing the law of armed conflicts" (1999)

   Course, "The international 'crimes' of States - a 'penal' responsibility of the State?" (2001)

- At the Academy of International Law, The Hague :

   Leader of the French-language seminars during the course on public international law (1985)

Inaugural Lecture of the public international law session (2007): "L'adaptation du droit international aux evolutions de la société internationale".

ACTIVITIES IN THE INTERNATIONAL LAW COMMISSION OF THE UNITED NATIONS :

Member (1990-2011)

Chairperson (1997-1998)

Member of the Drafting Committee (1991, 1993, 1994, 1995, 1996, 1998, 2000, 2001, 2003, 2007, 2008)

Chairman of the Working Group on the U.N. Decade for International Law (1992 - 1995)

Chairman of the Long Term Programme Group (2001-2006)

Chairman of the Working Group on the Unilateral Acts of States (1998-2006)

Chairman of the Working Group on The Obligation to Extradite or Prosecute (*aut dedere aut judicare*) (2008-2011)

Special Rapporteur on the topic : "Reservations to Treaties" (1994-2011)
> Preliminary Report, 1995, doc. A/CN.4/470 and Corr. 1 and 2, 78 p.
> Second Report, 1996, doc. A/CN.4/477 (24 p.) and Add. 1 (87 p.) and Corr. 1 and /CN.4/478 (23 p).
> Third Report, 1998, doc. A/CN.4/491 et Add.1 à 6.
> Fourth Report, 1999, doc. A/CN.4/
> Fifth Report, 2000, doc. A/CN.4/508 et Add. 1 and 2, 84p.; Add. 3 to 5
> Sixth Report, 2001, doc. A/CN.4/518 (9 p.) and Add. 1 to 3
> Seventh Report, 2002, A/CN.4/526 and Add. 1 to 4
> Eighth Report, 2003, A/CN.4/535 and Add.1
> Ninth Report, 2004, A/CN.4/544
> Tenth Report, 2005, A/CN.4/558 and Add. 1 and 2.
> Eleventh Report, 2006, A/CN.4/574.
> Twelfth Report, 2007, A/CN.4/584 et Add. 1.
> Thirteenth Report, 2008, A/CN.4/600.
> Fourteenth Report, 2009, A/CN.4/614 and Add.1 and 2.
> Fifteen Report, 2010, A/CN.4/624 and Add. 1 et 2.
> Sixteen Report, 2010, A/CN.4.626 and Add. 1.
> Seventeenth Report, 2011, A/CN.4/647 and Add. 1

ACTIVITIES AT THE INTERNATIONAL COURT OF JUSTICE :

Counsel and Advocate for Thailand in the case concerning the *Request for interpretation of the Judgment of 15 June 1962 in the case concerning the Temple of Preah Vihear (Cambodia v. Thailand)* (2011-present)

Counsel and Advocate for Japan in the case concerning *Whaling in the Antarctic* (2010-present)

Counsel and Advocate for Greece in the case concerning *Application of the Interim Accord of 13 September 1995* (2008-2011)

Counsel and Advocate for the Russian Federation in the case concerning the *Application of the International Convention on the Elimination of All Forms of Racial Discrimination* (2008-2011)

Counsel and Advocate for Peru in the case concerning *Maritime Delimitation between Chile and Peru* (2008-present)

Counsel and Advocate for Argentina in the case concerning *Certain Pulp Mills on the Uruguay River* (2006-2010)

Counsel and Advocate for Romania in the case concerning *Maritime Delimitation in the Black Sea* (2004-2009)

Counsel and Advocate for Singapore in the case concerning *Pedra Branca* (2003-2008)

Counsel and Advocate for Iran in the case concerning *Oil Platforms* (2002)

Counsel and Advocate for Benin in the case concerning the *Border Dispute* (2002-2005)

Counsel and Advocate for Liechtenstein in the case concerning *Certain Properties* (2001-2005)

Counsel and Advocate for India in the case concerning the *Aerial Incident of 10 August 1999* (2000)

Deputy Agent, Counsel and Advocate of the Republic of Guinea in the *Sadio Ahmadou Diallo* case (1999-2001)

Counsel and Advocate for Indonesia in the case concerning the *Sipadan and Ligitan Islands* (1997-2002)

Deputy Agent, Counsel and Advocate for Cameroon in the case concerning the *Land and maritime boundary* (1994-2003) and the *Request for Interpretation of the Judgment of 11 June 1998 in the case concerning the land and maritime boundary between Cameroon and Nigeria, Preliminary Objections* (Judgment of 25 March 1999)

Counsel and Advocate for Bosnia and Herzegovina in the cases concerning *Application of the Convention on the prevention and punishment of the crime of genocide* (1993-2007) and the *Request for Revision of the Judgment of 11 June 1996* (2001-2002).

Counsel and Advocate for Slovakia in the case concerning the *Gabčikovo-Nagymaros Project* (1993-present)

Deputy-Agent, Counsel and Advocate for Chad in the case concerning the *Territorial Dispute* (Judgment of 3 February 1994)

Counsel and Advocate for Australia in the cases concerning *Certain Phosphate Lands in Nauru* (Judgment of 26 june 1992) and *East Timor* (Judgment of 30 June 1995)

Counsel and Advocate for Burkina Faso in the *Frontier Dispute* case (Burkina Faso against Mali) (1984-1986); in the *Frontier Dispute* (Burkina Faso against Republic of Niger) (2010-present)

Counsel and Advocate for Nicaragua in the case concerning *Military and paramilitary activities in and against Nicaragua* (1986-1992), in the cases concerning *Border and transborder armed actions* (Nicaragua v. Costa Rica and Nicaragua against Honduras) (1986-1992) and in the cases concerning the *Maritime Delimitation between Honduras and Nicaragua* (2000-2007), the *Maritime Delimitation between Colombia and Nicaragua* (2001-present), the *River San Juan* (2005-2009) and *Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)* (2010-present).

Counsel for the French Republic in the case of the *Application for Review of Judgment n° 273 of the United Nations Administrative Tribunal* (*Mortished* case) (Advisory – 1982) and *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion – 2004) and Counsel and Advocate in the cases concerning the *Legality of the use by a State of nuclear weapons in armed conflict* (Request for an Advisory Opinion by the World Health Organization, 1994); the *Legality of the threat or use of nuclear weapons* (Request for Advisory Opinion by the General Assembly of the U.N., 1995); the *New Zealand's Request for an Examination of the Situation in accordance with Paragraph 63 of the Court's 1974 Judgment in the Nuclear Tests Case* (1995); *Legality of Use of Force (Serbia and Montenegro v. France)* (1999- 2005); *Certain Criminal Proceedings in France (Republic of the Congo v. France)* (2003-2010) and *Certain Questions of Mutual Assistance in Criminal Matters (Djibouti v. France)* (2006-2008) and *Accordance with International Law of the Unilateral Declaration of Independence by the Provisional Institutions of Self-Government of Kosovo* (2008-2010).

ACTIVITIES AT THE INTERNATIONAL TRIBUNAL FOR THE LAW OF THE SEA

- Counsel of Japan in case No. 14 (The *"Hoshinmaru"* Case (Japan v. Russian Federation), Prompt Release*)* and 15 (The *"Tomimaru"* Case (Japan v. Russian Federation), Prompt Release) (2007);

- Counsel and Advocate of Myanmar in case No. 16 (*Dispute concerning delimitation of the maritime boundary between Bangladesh and Myanmar in the Bay of Bengal*) (2010-2011).

ACTIVITIES IN ARBITRATION MATTERS

Participation in various cases as an arbitrator, a counsel and advocate or a consultant in ICSID, ICC and PCA cases (current cases are omitted).

Designated to the Panel of Arbitrators of the International Centre for the Settlement of Investment Disputes (ICSID) by the Chairman of the Administrative Council (2011-present)

Alternate Arbitrator, Arbitration and Conciliation Court of the OSCE (2001-present)

Permanent Court of Arbitrage cases:

- Counsel and lawyer of France in the *Eurotunnel* case(2005-2010);

- Counsel and lawyer of Sudan in the *Abyei* case (2008-2009).

ICSID cases:

- Expert mandated by the defendant in the case *E.T.I. Euro Telecom International N.V. v. Plurinational State of Bolivia* (ARB/07/28) (2009);

- Expert mandated by the defended in the case *Hulley Enterprises Ltd., Yukos Universal Ltd., Veteran Petroleum Ltd* (decision on jurisdiction) (2008-2010);

- Expert mandated by the plaintiff in the case *Brandes Investment Partners, LP v. Bolivarian Republic of Venezuela* (ARB/08/3) (2008-present);

- Consultant for the Republic of the Philippines in the case *Fraport AG Frankfurt Airport Services Worldwide v. Republic of the Philippines* (ARB/03/25) (2008-2009);

- Appointed Arbitrator by Argentina in the case of *Mobil Exploration and Development Argentina Inc., Suc. Argenina S.S. v. Republic of Argentina* (ICSID ARB/04/16) (2005)

Various arbitration cases:

- Counsel and lawyer for the Republic of Chad in the case *SOFRECO v. Republic of Chad* (EDF) (2009-2011)

- Arbitrator designated by Eutelsat in the case *Eutelsat S.A. v. Georgia* (*ad hoc* arbitration – friendly settlement) (2007-2008);

- Counsel and lawyer for the Kyrgyz Republic in the case *Oxus Gold PLC v. Kyrgyz Republic* (UNCITRAL) (2006-2008);

- Appointed Arbitrator by Argentina in the case *Banka of Nova Scotia v. Argentine* (UNCITRAL – suspended) (2005).

OTHER ACTIVITIES :

Numerous legal consultations on administrative law and international law at the request of various authorities in France and abroad (French and foreign Ministries of Foreign Affairs), public and semi-public bodies and international organizations (UNESCO and various other organizations; Federation of International Civil Servants Associations (FISCA), staff associations of several international organizations, United Nations University) and private companies.

Associate Consultant, LYSIAS Advocates (Paris) (1993 - 2007)

Consultant-Expert to the Arbitration Commission of the International Conference on Yugoslavia ("Badinter Commission") (1991 - 1993)

Rapporteur of the French Committee Jurists on the Creation of an International Criminal for Former Yugoslavia ("TRUCHE Commission") (1993)

Member of the French Delegation to the E.C.S.C. (Helsinki, 1992, Geneva, 1992)

Legal Adviser of the World Tourism Organization (W.T.O. - Madrid) (1990 -   )

Independent Objector (Internet Corporation for Assigned Names and Numbers - ICANN) for generic top level domain names (new gTLD) (2012 -   )

Alternate member of the Sub-Commission on Prevention of Discrimination and Protection of Minorities, United Nations Commission on Human rihgts (1983 - 1991)

Member of the French delegation at the GATT ministerial session (Geneva, 1982), at UNCTAD VI (Belgrade, 1983) and a number of sessions of the Trade and Development Board

Adviser to the French representative on the Working Group of Governmental Experts on the Right to Development, set by the United Nations Commission on Human Rights (1981)

Government expert at the UNESCO Congress on Education for Disarmament (June 1980). Report on "Disarmament in the teaching of international questions". Consultant on the same subject (August 1981)

From 1969 to 1975, served on the staff of an Advocate to the Council of State and the Court of Cassation (drafting written procedural documents for applications to the Council of State and to administrative tribunals)

President of the French Association for Disarmarment Research and Studies (AFRED) (1979-1982)

President of the Association for the study of external legal policies (POJUREX) (1987 -   )

Director (with P. Daillier), "International and European Law Library" (L.G.D.J. - Montchrestien publishers).

Director (with P.-M. Eisemann), collection "International Law", Economica Publishers.

Member, Board of Editors of the *Annuaire français de Droit Internationa*

Member, Advisory Board, *European Journal of International Law*

Member, Board of the Editors, *International Criminal Law Review*

Member, Honorary Board, *Romanian Journal of International Law*

Member, Editorial Board, *Miskolć Journal of International Law*

Member, Scientific Council, *Annales de Droit* (Rouen)

Member, Advisory Board, Amsterdam Centre for International Law

DECORATIONS :

Légion d'honneur (Knight, France - 1998)

Palmes académiques (France) (Knight, 1986; Officer 2007)

Knight Romanian National Order "Serviciul Credincios" (Romania, 2009).

Order of the Double White Cross (Slovakia, 2006)

Commander, Ordre de la valeur (Cameroon, 2003)

Officer, Order of merit (Chad, 1995)

Gold Star of Nahouri (Burkina Faso, sylver medal, 1987)

Associate of the Institut de Droit international (2007)

Docteur *honoris causa* de l'Université Estácio de Sá (Rio de Janeiro - 1998), de l'Université de Miskolć (Hongrie - 2000), et de l'Académie russe du Commerce extérieur (Moscou - 2002) et de la Faculté de Droit d'Athènes (2011).

Member of the Institute of International Public Law and International Relations of Thessaloniki (Greece, 2001)

René Maheu Prize for the International Civil Service, Special award (1995)

Medal of the Faculty of Law of Granada (Spain, 1992)

Lemonon prize of the Institute of France (Moral and Political Sciences Academy) for the book on the *United Nations Charter* (with J.P. Cot - 1986)

RESEARCH AND PUBLICATIONS :

Books (as author or editor):

-   *The Law of International Responsibility* (with James Crawford & Simon Olleson), Oxford University Press, 2010, 1296 p. Edition française à paraître en 2011 aux éditions Pedone (with James Crawford, Sandra Szurek & Pierre Bodeau-Livinec).

-   *Actualité du droit des fleuves internationaux*, Actes des journées d'étude franco-roumaines (ADIRI/CEDIN), 23-24 October 2008 (with Bogdan Aurescu), Pedone, 2010, 310 p.

-   *Droit international public* (with Patrick Daillier & Mathias Forteau), LGDJ, Paris, 8th edition, 2009, 1709 p. (7th edition, 2002, 1510 p.; 6th edition, 1999, 1457 p., 5th edition, 1994, 1379 p.; 4th edition, 1992, 1269 p.; 3rd édition 1988, 1189 p.; 2nd edition, 1979, 994 p.; supplement with update of 1st edition by Nguyen Quoc Dinh, 1977, 132 p.); partial publication in Greek (by H. Dipla, *Δημοσιο Διεθνες Δικαιο*, *Το Δικαιο της Θαλασσας*, Papaxisis, Athens, 1991, 160 p.) and in Hungarian (by P. Kovács, *Nemzetközi Közjog*, Osiris, Budapest, 1997, 566 p.); translations in Portuguese, Gulbenkian Foundation, Lisbon, 2000, 1230p.; 2nd ed. 2005, 1517 p., and in Russian, 2004, 2 vols., Sphera Publishers (Kiev).

-   *International Law Between Universalism and Fragmentation – Festschrift in Honour of Gerhard Hafner*, (co-ed. with I. Buffard, J. Crawford et St. Wittich), Nijhoff, Leiden-Boston, 2008, xlvi-1083 p.

-   *La Charte des Nations Unies, Constitution mondiale?* (co-ed. with Régis Chemain), actes du colloque du CEDIN, Cahiers internationaux n° 20, Pedone, 2006, 237 p.

-   *La Charte des Nations Unies* (co-edited with Jean-Pierre COT), Economica, Paris, 1985; 2nd edition 1991, XIV-1,571 p.; preface by Mr. J. Pérez de Cuéllar (work awarded the Lemonon Prize of the Institut de France, Academy of Moral and Political Sciences); 3rd ed. 2005, XV-2363 p., preface by Mr. Kofi Annan; translations into Japanese (1993) and English (to appear in 2006); commentaries of the Preamble and Article 55.

-   *Droit international pénal*, ed. (with Hervé ASCENSIO and Emmanuel DECAUX), Paris, Pedone, 2000, XVI-1053 p.

-   *Le droit international du développement social et culturel* (ed., with Jean-Marc Sorel), Acts of the Round Table organized by the Faculty of Law of the University of Paris-North, 11-12 May 1990, L'Hermès, Paris, 1997, 408 p.

-   *Les fonctionnaires internationaux* (with David Ruzié), PUF, Paris, "Que sais-je ?" n°2762, 1993, 128 p.

- *Le droit international du développement*, Paris, PUF, "Que sais-je ?", n°1731, 2nd edition, 1987, 128 p., 1st edition, 1978. Japanese translation 1989.

- *Droit international public*, PUF, Memento Themis, Paris, 1981, 154 p. Translation in Japanese, 1992.

- *Le cadre juridique de la vie économique internationale*, duplicated lecture notes (Institute of Political Studies, Paris, 1981 - 1982); fasc. I : *Droit et économie internationale, le droit des relations monétaires internationales*, 322 p., updated 1982 - 1983.

- *Les voies de recours ouvertes aux fonctionnaires internationaux*, Pédone (extract from the *Revue Générale de Droit International Public*), 1982, 202 p.

- *Répertoire de la jurisprudence des tribunaux administratifs internationaux*, prepared at the request of FICSA, vol. II, *Le droit procédural*, United Nations, 1987, 1, 304 p., vol I, *Le droit applicable*, 1988, 528 p., and vol. III, *Le droit substantiel*.

- *Recherche sur les principes généraux de droit en droit international public*, Doctoral thesis, Paris II, 1974 (examining board: S. Bastid, Chairwoman, P. Reuter, M. Virally), 504 p.

Case-books :

- *Les Nations Unies - Textes fondamentaux*, P.U.F., coll. "Que sais-je ?", n°3035, 1995, 128 p.

- *Droit d'ingérence ou devoir d'assistance humanitaire?*, *Problèmes politiques et sociaux*, n°758-759, 1-22 Dec. 1995, La documentation française, 133 p.

Forewords:

- A. Ben Mansour, *La Mise en oeuvre des arrêts et sentences des juridictions internationales*, Larcier, 2011, 622 p.

- A. Beaudoin, *Uti possidetis et sécession*, Dalloz-Sirey, 2011, 667 p.

- M. Montjoie, *Droit international et gestion des déchets radioactifs*, L.G.D.J.-Lextenso, Paris, 2011, xvi-395 p.

- C. Bories, *Le patrimoine culturel en droit international – Les compétences des Etats à l'égard des éléments du patrimoine culturel*, Pedone, Paris, 2011, 556 p.

- *The Law of International Responsibility* (J. Crawford, A. Pellet, S. Olleson eds), Oxford University Press, 2010, v-1296 p.

- B. Tchikaya, *Mémento de la jurisprudence du droit international public*, Hachette Supérieur, Paris, 2010, 160 p.

- N. Kreipe, *Les autorisations données par le Conseil de sécurité des Nations Unies à des mesures militaires*, L.G.D.J., 2009, XII-321 p.

- A.-L. Vaurs-Chaumette, *Les sujets du droit international pénal – Vers une nouvelle définition de la personnalité juridique internationale ?*, Pedone, Paris, 2009, IX-545 p.

- J. Fouret and D. Khayat, *Recueil des commentaires des décisions du CIRDI (2002-2007)*, Bruylant, Bruxelles, 2009, XXIV-710 p.

- N. Susani, *Le règlement des différends dans le Mercosur - Un système de droit international pour une organisation d'intégration*, L'Harmattan, Paris, 2008, 324 p.

- H. Lesaffre, *Le règlement des différends au sein de l'OMC et le droit de la responsabilité internationale*, L.G.D.J., Paris, 2007, XVII-614 p.

- F. Latty, *La* lex sportiva *– Recherche sur le droit transnational*, Nijhoff, Leiden/Boston, 2007, XX-849 p.

- M. Forteau, *Droit de la sécurité collective et droit de la responsabilité internationale de l'État*, Pedone, Paris, 2006, vi-699 p.

- V. Rodriguez Cedeño e Milagras Betancourt C., *Temas de Derecho Internacional VII – Introducción al Estudio de Derecho de los Tratados y de los Actos Jurídico Unilaterales de los Estados*, Caracas, 2004, XXIII-265 p.

- G. Guillaume, *La Cour internationale de Justice à l'aube du XXIème siècle – Le regard d'un Juge*, avec R. Abraham, Pedone, 2003, 331 p.

- L. Nemer Caldeira Brant, *A autoridade da coisa julgada no direito internacional público*, Forense, Rio de Janeiro, 2002, XVIII-510 p et *L'autorité de la chose jugée en droit international public*, L.G.D.J., 2003, XI-396 p.

- P.-H. Ganem, *Sécurisation contractuelle des investissements internationaux - Grands projets (Mines, énergie, métallurgie, infrastructures)*, FEC/Bruylant, Paris/Bruxelles, 1997, 906 p.

- P. Boniface, *Les sources du désarmement*, Économica, 1989, 263 p.

Articles on international law:

- "The Effects of Palestine's Recognition of the International Criminal Court's Jurisdiction", *in* C. Meloni and G. Tognoni (eds.), *Is There a Court for Gaza? A Test Bench for International Justice*, T.M.C. Asser Press, The Hague, The Netherlands, 2012, pp. 409-428.

- "The *Nicaragua* Case: 'Mafiosi's' and 'Veteran's' Approaches Combined", *Leiden Journal of International Law* (2012), 25, pp. 481-489.

- "Reservations to Human Rights Treaties : Not an Absolute Evil...", with Daniel Müller, *in From Bilateralism to Community Interest – Essays in Honour of Judge Bruno Simma*, Oxford University Press, 2011, pp. 521-551.

- "Reservations to Treaties: An Objection to a Reservation is Definitely not an Acceptance", with Daniel Müller, *in* Enzo Cannizzaro (ed.)., *The Law of Treaties Beyond the Vienna Convention*, Oxford University Press, 2011, pp. 37-59.

- "Peaceful Settlement of International Disputes", *in* Rüdiger Wolfrum (dir.), Max Planck Encyclopedia of Public International Law, Oxford UP, à paraître ; disponible en ligne [available on line] (http://www.mpepil.com/).

- Articles 19 and 22 and, with William Schabas, article 23 (Reservations) *in* Olivier Corten et Pierre Klein, dirs., *The Vienna Convention on the Law of Treaties – A commentary*, Oxford University Press, vol. 1, 2011, pp. 405-488, 568-593 and 594-627.

- "Article 42 of the 1951 Convention / Article VII of the 1967 Protocol", *in* Andreas Zimmermann ed.,*The 1951 Convention Relating to the Status of Refugees and its 1967 Protocol - A Commentary*, Oxford U.P., 2011, pp. 1615-1639.

- Afterwords to Régis Chemain (dir), colloque du CEDIN, *La refondation du système monétaire et financier international – Evolutions réglementaires et institutionnelles*, Pedone, 2011, pp. 347-356.

- Conclusions générales in S.F.D.I., colloque d'Orléans, *L'eau en droit international*, Pedone, 2011, pp. 395-402.

- "Les techniques interprétatives de la norme internationale" (Forewords), *R.G.D.I.P.*, 2011 n° 2, pp. 291-295.

- "Shaping the Future in International Law : The Role of the World Court in Law-Making" *in Looking to the Future – Essays on International Law in Honor of W. Michael Reisman*, Martinus Nijhoff, Leiden/Boston, 2010, pp. 1065-1083.

- "The Palestinian Declaration and the jurisdiction of the International Criminal Court", Journal of International Criminal Justice, 2010, vol. 8, pp. 981-999; also published in Al-Zaytouna Centre for Studies & Consultations (Beirut), *Israel and international Law*, Beirut, 2010, pp. 379-406; and in French (with some changes and additions): "Les effets de la reconnaissance par la Palestine de la competence de la Cour pénale international", *Mélanges en l'honneur de Madjid Benchikh – Droit, liberté, paix, développement*, Pedone, Paris, 2011, pp. 327-344.

- "The ILC's Articles on State Responsibility for Internationally Wrongful Acts and Related Texts" *in* J. Crawford, A. Pellet, S. Olleson eds., *The Law of International Responsibility*, Oxford University Press, 2010, pp. 75-94.

- "The Definition of Responsibility in International Law" *in* J. Crawford, A. Pellet, S. Olleson eds., *The Law of International Responsibility*, Oxford University Press, 2010, pp. 3-16.

- "Les problèmes posés par l'alluvionnement" *in* B. Aurescu et A. Pellet dir., *Actualité du droit des fleuves internationaux* (Actes des journées d'étude franco-roumaines (ADIRI/CEDIN) des 23-24 octobre 2008), Pedone, 2010.

- "Remarques sur l'(in)efficacité de la Cour internationale de Justice et d'autres juridictions internationales" *in Liber Amicorum Jean-Pierre COT - Le procès international*, Bruylant, Bruxelles, 2009, pp. 193-213.

- "Adieu Philippines – Remarques sur la distinction entre les réclamations conventionnelles et contractuelles dans le droit de l'investissement international" *in Le droit international économique à l'aube du XXIème siècles - Mélanges offerts à Dominique Carreau et Patrick Juillard*, Pedone, Paris, 2009, pp. 97-110.

- "Les rapports de systèmes après l'affaire *Kadi* – Constitutionnalisation du droit des Nations Unies ou triomphe du dualisme ?", *Revue du Marché commun et de l'Union européenne*, juin 2009, pp. 415-418.

- « Le recours à la force, le droit et la légitimité – Notes sur les problèmes posés par le principe de l'interdiction du recours à la force armée en cas de carence du Conseil de sécurité », *Frieden in Freiheit, Peace in liberty, Paix en liberté – Festschrift für Michael Bothe zum 70.* Geburstag, 2008, pp. 249-268.

- « Force and the Settlement of Political Disputes: The Debate" (debate with Michael Glennon) *in* Y. Daudet ed., *Topicality of the 1907 Hague Conference, The Second Peace Conference*, Colloquium of The Hague Academy of International Law (6-7 Sept. 2007), Nijhoff, Leiden/London, 2008, pp. 225-249.

- "The Anatomy of International Courts and Tribunals", *L.P.I.C.T.* 2008, n° 3, pp. 275-287.

- "Anglo-Saxon and Continental Approaches to Pleading Before the ICJ" (with J. Crawford), in *International Law Between Universalism and Fragmentation – Festschrift in Honour of Gerhard Hafner*, Nijhoff, Leiden-Boston, 2008, pp. 831-867.

- "L'adaptation du droit international aux besoins changeants de la société internationale" - inauguration lecture, *Recueil des cours* 2007, vol. 329, Nijhoff, Leiden/Boston 2008, pp. 9-47.

- "Lotus que de sottises on profère en ton nom!: remarques sur le concept de souveraineté dans la jurisprudence de la Cour mondiale", *Mélanges en l'honneur de Jean-Pierre Puissochet : l'État souverain dans le monde d'aujourd'hui*, Pedone, Paris, 2008, p. 215-230.

- "Legitimacy of Legislative and Executive Actions of International Institutions" in R. Wolfrum and V. Röben eds., *Legitimacy in international Law*, Springer, Berlin, 2008, pp. 63-82.

- "Cours Général : Le droit international entre souveraineté et communauté internationale – La formation du droit international", *Anuário Brasileiro de Direito Internacional*, vol. II, 2007, pp. 12-74.

- "Le renforcement du rôle de la C.I.J." in Yves Sandoz ed., *Quel droit international pour le 21ème siècle ?* (actes du colloque de Neuchâtel), Bruylant, Bruxelles, 2007, pp. 134-143.

- "La seconde mort d'Euripide Mavrommatis ? Notes sur le projet de la C.D.I. sur la protection diplomatique", *Droit du pouvoir, pouvoir du droit – Mélanges offerts à Jean Salmon*, Bruylant, Bruxelles, 2007, pp. 1359-1382.

- "Comments in Response to Christine Chinkin and in Defense of *jus cogens* as the Best Bastion against the Excesses of Fragmentation", *Finnish Yearbook of International Law*, 2006, pp. 83-90.

- "Le droit international dans l'ombre de l'Empire", Proceedings of the Inaugural Conference of the European Society of International Law, *Baltic Yearbook of International Law*, 2006, pp. 27-36.

- "Le projet d'articles de la C.D.I. sur la protection diplomatique: une codification pour (presque) rien", in Marcelo G. Kohen ed., *Promoting Justice, Human Rights and Conflict Resolution through International Law* – Liber Amicorum *Lucius Caflisch*, Brill, Leiden, 2007, pp. 1133-1155.

- Articles 19 et 22 and, with William Schabas, article 23 (Reservations) *in* Olivier Corten et Pierre Klein, eds., *Les Conventions de Vienne sur le droit des traités – Commentaire article par article*, Bruylant, Bruxelles, 2006, vol. I, pp. 639-796, 934-970 et 971-1022.

- "Vous avez dit 'monisme'? – Quelques banalités de bon sens sur l'impossibilité du prétendu monisme constitutionnel à la française", *L'architecture du droit – Mélanges en l'honneur de Michel Troper*, Economica, Paris, 2006, pp. 827-857.

- "Remarks on Proceedings before the International Court of Justice" *in* A. del Vecchio ed., New International Tribunals and New International Proceedings, Giuffrè, Milano, 2006, pp. 99-118 and in *The Law and Practice of International Courts and Tribunals*, 2006, pp. 163-182.

- "Les voies d'un ordre mondial", avec M. Delmas-Marty et P. Lamy, *Le débat*, novembre-décembre 2006, pp. 4-18.

- "Article 38" *in* A. Zimmermann, Ch. Tomuschat and K. Oellers-Frahm, *The Statute of the International Court of Justice : a Commentary*, Oxford UP, 2006, pp. 677-792.

- "Unity and Diversity with Regard to International Treaty Law", Comment, *in* A. Zimmermann and R. Hofmann (eds.), *Unity and Diversity in International Law (Proceedings of an International Symposium of the Kiel Walther Schücking Institute of International Law, November 4-7, 2004)*, Duncker & Humblot, Berlin, 2006, pp. 247-251.

- Ch. Tomuschat and J.-M. Thouvenin (eds.), *The Fundamental Rules of the International Legal Order* – Jus Cogens *and Obligations* Erga Omnes (conclusions), Nijhoff, Leiden/Boston, 2005, pp. 417-424.

- "Complementarity of International Treaty Law, Customary Law, and Non-Contractual Law Making" *in* R. Wolfrum and V. Röben, *Developments of International Law in Treaty-Making*, Springer, Berlin, 2005, pp. 409-415.

- "Les nouvelles tendances du droit international. Aspects 'macro-juridiques'", *Études internationales* (Tunis) n° 92, 3/2004, pp. 62-82.

- Postface: "Internationalized Criminal Courts: Better Than Nothing…" *in* Cesare P.R. Romano, André Nollkampfer and Jann K. Kleffner eds., *Internationalized Criminal Courts and Tribunals*, Oxford U.P., 2004, pp. 437-444.

- "Strengthening the Role of the International Court of Justice as the Principal Judicial Organ of United Nations", *The Law & Practice of International Courts and Tribunals*, 2004, pp. 159-180 (translated and updated version of : "Le renforcement du rôle de la Cour en tant qu'organe judiciaire principal des Nations Unies" *in* Gregory Peck and Roy S. Lee eds., *Increasing the Effectiveness of the International Court of Justice - Proceedings of the ICJ/UNITAR Colloquium to Celebrate the 50th Anniversary of the Court*, Nijhoff/ Unitar, 1997, pp. 235-253).

"Can a State Victim of a Terror Act Have Recourse to Armed Force? ", *Humanitäres Völkerrecht*, 2/2004, pp. 68-72 (with Vladimir Tzankov); in French: "L'État victime d'un acte terroriste peut-il recourir à la force armée?" *in* S.F.D.I. and Deutsche Gesellschaft für Völkerrecht, *New Threats to International Peace and Security*, Pedone, Paris, 2004, pp. 95-107 (summaries in English and German).

- Communication: "Le rôle et la place du droit international dans la pratique- le point de vue des praticiens; la pratique dans les travaux de la C.D.I. " *in* S.F.D.I., colloque de Genève, *La pratique et le droit international*, Paris, Pedone, 2004, pp. 259-263.

- "Between Codification and Progressive Development of the Law: Some Reflections from the ILC", *International Law Forum* 2004, pp. 15-24.

- "Inutile Assemblée générale?", *Pouvoirs*,n° 109, 2004, pp. 43-59.

- "The Charter of the United Nations: A Commentary of Bruno Simma's Commentary", *Michigan Journal of International Law*, 2004, vol. 25, n° 1, pp. 135-151.

- "Le crime international de l'État – Un phoenix juridique" *in The New International Criminal Law – Thesaurus Acroasium*, 2001 International Law Session, vol. XXXII, Sakkoulas Publications, Athens-Thessaloniki, pp. 281-351.

- "Can International Law Survive US Leadership? ", *Austrian Review of International and European Law*, 2003, pp. 101-108.

- "Law of Treaties" (comments) *in* M. Byers and G. Nolte ed., *United States Hegemony and the Foundations of International Law*, Cambridge U.P., 2003, pp. 418-422.

- "Les réserves aux conventions sur le droit de la mer" *in La mer et son droit – Mélanges offerts à Laurent Lucchini et Jean-Pierre Quéneudec*, Pedone, Paris, 2003, pp. 501-520.

- "Les articles de la C.D.I. sur la responsabilité de l'État pour fait internationalement illicite; suite – et fin?", *A.F.D.I.* 2002, pp. 1-23.

- "Les rapports de Roberto Ago à la C.D.I. sur la responsabilité des États", *International Law Forum*, 2002, pp. 222-229.

- "La competencia material y el derecho applicable en el estatuto de la Corte penal internacional" *in* Instituto Pedro Gual, Serie Cuadernos 2, *Promoción y Protección Internacional de la Persona*, Caracas, 2002, pp. 51-57.

- "The New Draft Articles of the International Law Commission on the Responsibility of States for International Wrongful Acts: A *Requiem* for States' Crimes?", *Netherlands Yearbook of International Law*, 2001, pp. 55-79 (in French: "Le nouveau projet de la C.D.I. sur la responsabilité de l'État pour fait internationalement illicite: *Requiem* pour le crime?" *in Man's Inhumanity to Man – Festschrift Antonio Cassese*, Kluwer, The Hague, 2002, pp. 654-681).

- "La C.I.J. et les réserves aux traités – Remarques cursives sur une révolution jurisprudentielle" *in* Liber Amicorum *Judge Shigeru Oda*, Kluwer, The Hague, 2002, pp. 481-514.

- "Entry Into Force and Amendment of the Statute" *in* A. Cassese, P. Gaeta and J.R.W.D. Jones eds., *The Rome Statute of the International Criminal Court: A Commentary*, Oxford U.P., 2002, pp. 145-184; "Applicable Law", *ibid.*, pp. 1051-1084 and "Settlement of Disputes", *ibid.*, pp. 1841-1848.

- with Sarah Pellet, "The Aftermath of September 11", *Tilburg Foreign Law Review*, vol. 10, n° 1, pp. 64-75.

- "La terreur, la guerre, l'ONU", *in* "Les nouvelles formes du terrorisme international et leur impact sur l'évolution du droit international", Université de Miskolc, *European Integration Studies*, vol. I, 2002, pp. 13-18; in Portuguese: "Terrorismo e Guerra. O Que Fazer das Nações Unidas?" *in* L. Nemer Caldeira Brant ed., *Terrorismo e Direito*, Forense, Rio de Janeiro, 2003, pp. 173-182.

- "L'imputabilité d'éventuels actes illicites - Responsabilité de l'OTAN ou des États membres?", in Ch. Tomuschat ed., *Kosovo and the International Community - A Legal Assesment*, Kluwer, The Hague, 2002, pp. 193-202.

- "'Human Rightism' and International Law", *Italian Yearbook of International Law*, 2000, pp. 3-16 (English translation of the « Gilberto Amado Lecture » as made in the United Nations (Geneva) on 18 July 2000 on « 'Droits de l'hommisme' et droit

international » (http://untreaty.un.org/ilc/sessions/52/french/amado.pdf - also available in *Droits fondamentaux*, http://www.droits-fondamentaux.org/article.php3?id_article= 27.

- "La codification du droit de la responsabilité internationale: Tâtonnements et affrontements", *in* L. Boisson de Chazournes and V. Gowlland-Debbas eds., *The International Legal System in Quest of Equity and Universality,* Liber Amicorum *Georges Abi-Saab*, Kluwer, The Hague, 2001, pp. 285-304.

- "Le procès international et le temps - Le temps du Conseil" *in* S.F.D.I., Colloque de Paris, 2000, *Le droit international et le temps* (conclusions) , Pedone, Paris, 2001, pp. 243-248.

- "La *lex mercatoria*, 'tiers ordre juridique'? Remarques ingénues d'un internationaliste de droit public" *in Souveraineté étatique et marchés internationaux à la fin du 20ème siècle – Mélanges en l'honneur de Philippe Kahn*, Litec, 2000, pp. 53-74.

- "La responsabilité pénale individuelle, alternative aux sanctions collectives?" *in* V. Gowlland Debbas ed., *United Nations Sanctions and International Law*, Kluwer, The Hague, 2000, pp. 105-116.

- "A French Constitutional Perspective on Treaty Implementation" *in* Thomas M. Franck ed., *Delegating State Powers: The Effects of Treaty Regimes on Democracy and Sovereignty*, Transnational Publishers, 2000, pp. 279-293.

- "Brief Remarks on the Unilateral Use of Force", *E.J.I.L.* 2000, pp. 385-392.

- "The Role of the International Lawyer in International Litigation" *in* Ch. Wickremasinghe ed., *The International Lawyer as Practionner*, B.I.I.C.L., London, 2000, pp. 147-162.

- "State Sovereignty and the Protection of Fundamental Human Rights: An International Law Perspective", Pugwash Occasional Papers, vol. 1, N° 1, Feb. 2000, pp. 37-45.

- "Responding to New Needs through Codification and Progressive Development" (Keynote Address), *in* V. Gowlland-Debbas ed., *Multilateral Treaty-Making: The Current Status of Challenges to and Reforms Needed in International Legislative Process*, Kluwer, The Hague, 2000, pp. 13-23.

- "'La guerre du Kosovo' – Le fait rattrapé par le droit", *International Law Forum*, vol. 1, n° 3, 1999, pp. 160-165.

- "La C.P.I. - Compétence matérielle et modalités de saisine", *in La Cour pénale internationale : colloque Droit et démocratie*, Documentation Française, Paris, 1999, pp. 41-54.

- "Can a State Commit a Crime? Definitely, Yes!", *E.J.I.L.* 1999, vol. 10, n° 2, pp. 425-434.

- "La Commission du Droit international, pour quoi faire?", *Boutros Boutros-Ghali* Amicorum Discipulorumque Liber – *Paix, développement, démocratie*, Bruylant, Bruxelles, 1998, pp. 583-612.

- "Pour la Cour pénale internationale quand même! - Quelques remarques sur sa compétence et sa saisine", *L'Observateur des Nations Unies*, n° 5, 1998, pp. 143-163; also published and updated in *International Criminal Law Review*, 2001, pp. 91-110..

- "L'unité ou la fragmentation du système juridique international" in S.F.D.I., colloque de Strasbourg, *La protection des droits de l'homme et l'évolution du droit international*, Pedone, Paris, 1998, pp. 294-298.

- "Le droit international à l'aube du XXIème siècle (La société internationale contemporaine - permanences et tendances nouvelles)", Fundamental Course, *in Bancaja Euromediterranean Courses of International Law*, vol. I, 1997, Aranzadi, Pamplona, 1998, pp. 19-112.

- "The Role of the International Lawyer in International Litigation", in Ch. Wickremasinghe ed., *The International Lawyer as Practionner*, B.I.I.C.L., London, 2000, p. 147-162; in French: "Conseil devant la Cour internationale de Justice - Quelques impressions", *in Mélanges offerts à Hubert Thierry*, Pedone, Paris, 1998, pp. 345-362, also published and updated under the title: "Remarques sur le 'métier' de Conseil devant la Cour internationale de Justice", *in* Nations Unies, *Collection of Essays by Legal Advisers of International Organizations and Practitioners in the Field of International Law*, New York, 1999, sales n° E/F/S.99.V.13, pp. 435-458.

- CEDIN Paris X, *Perspectives d'intégration des pays d'Europe centrale et orientale aux institutions de l'Europe occidentale*, Montchrestien, Paris, 1998, general conclusion, pp. 371-380.

- "Le Conseil constitutionnel, la souveraineté et les traités - À propos de la décision du Conseil constitutionnel du 31 décembre 1997 (traité d'Amsterdam)", *Les Cahiers du Conseil constitutionnel*, n° 4, 1998, pp. 111-120.

- "Individual Rights, Minority Rights, and Group Rights", *in* Ernest R. May and Ageliki E. Laiou eds., *The Dumbarton Oaks Conversations and the United Nations, 1944-1994*, Dumbarton Oaks Research Library, Washington D.C., 1998, pp. 105-109.

- CEDIN Paris X, *Sanctions unilatérales, mondialisation du commerce et ordre juridique international - À propos des lois Helms-Burton et D'Amato-Kennedy*, Montchrestien, Paris, 1998, Conclusions, pp. 321-334.

- "Vive le crime! Remarques sur les degrés de l'illicite en droit international" *in* I.L.C., Alain Pellet ed., *International Law at the Dawn of the Twenty-First Century - Views from the I.L.C.*, United Nations, New York, 1997, pp. 287-315.

- "Le projet de Statut de Cour criminelle internationale permanente - Vers la fin de l'impunité?", in *Héctor Gros Espiell* Liber Amicorum, Bruylant, Bruxelles, 1997, pp. 1057-1085.

- "Remarques sur une révolution inachevée - Le projet de la C.D.I. sur la responsabilité des États", *Annuaire français de droit international* 1996, pp. 7-32.

- "Harmonie et contradiction de la justice internationale" in, Rafâa BEN ACHOUR et Slim LAGHMANI dirs., Rencontres internationales de la Faculté des Sciences juridiques de Tunis, *Harmonie et contradictions en droit international*, Pédone, Paris, 1996, pp. 195-214.

- "Quelle Cour criminelle internationale?", *Témoin*, n° 7, Fall 1996, pp. 197-206. Revised version: *La Lettre de Juristes sans frontières*, déc. 1996, pp. 2-5.

- "Les fondements juridiques internationaux du droit communautaire", Academy of European Law, Florence, *Recueil des cours*, vol. V, book 2, Nijhoff, Dordrecht, 1997, pp. 193-271.

- "Mondialisation du droit international?", *Après-demain*, avril-mai 1996, pp. 37-39; also published and updated *in* Serge Cordellier dir., *La mondialisation au-delà des mythes*, La Découverte, coll. "L'état du monde", 1997, pp. 93-100; 2nd revised ed., 2000, pp. 93-100.

- "L'activité du Tribunal pénal international pour l'ex-Yougoslavie", (with Hervé ASCENSIO), *Annuaire français du droit international* 1995, pp. 101-136.

- "La juridiction pénale internationale de Nuremberg à La Haye", *Le Monde Juif, Revue d'histoire de la Shoah*, 1996, n° 156, pp. 92-104.

- "The Road to Hell is Paved with Good Intentions - The United Nations as Guarantor of International Peace and Security : a French Perspective" *in* Christian Tomuschat, ed., *U.N. at Age Fifty*, Nijhoff, Drodrecht, 1995, pp. 113-133.

- "La formation du droit international dans le cadre des Nations Unies", *European Journal of International Law*, 1995, pp.401-425.

- "The International Court of Justice and the Political Organs of the United Nations - Some Further but Cursory Remarks", in F. SALERNO ed., *Il ruolo del giudice internazionale nell'evoluzione del diritto internazionale e communitario - Atti del Convegno di Studi in Memoria di Gaetano Morelli*, CEDAM, Milan, 1995, pp.115-124.

- "Les problèmes découlant de la création et de la dissolution des Etats et les flux de réfugiés", in V. GOWLLAND-DEBBAS ed., *The Problem of Refugees in the Light of Contemporary International Law Issues, Kluwer*, 1995, pp. 51-57.

- S.F.D.I., Paris Symposium, 1994, *Les juridictions administratives internationales et le contentieux de la fonction publique internationale*, Conclusions of the Symposium, Pédone, Paris, 1995, pp.253-259.

- "50 ans de Nations unies - 50 ans de droit international" in U.N. Center of Information, Paris, "Spécial 50è anniversaire de l'ONU", pp.11-20.

- "Peut-on et doit-on contrôler les actions du Conseil de sécurité ?" S.F.D.I., Symposium of Rennes, *Le chapitre VII de la Charte des Nations Unies et les nouveaux aspects de la sécurité collective*, Pedone, 1995, pp. 221-238.

- "Quel avenir pour le droit des peuples à disposer d'eux-mêmes ?", Liber Amicorum *Jimenez de Arechaga*, Fundacion de cultura universitaria, Montevideo, 1994, pp. 255-276.

- "Le Tribunal criminel international pour l'ex-Yougoslavie - poudre aux yeux ou avancée décisive ?" *Revue générale de droit international public*, 1994, pp. 7 - 60.

- "Nationalités et minorités dans l'ancienne Yougoslavie - Quelques aspects juridiques", in *La Méditerranée, espace de coopération*? collective book in honour of Professor Maurice Flory, Pedone, 1994, pp. 143-152, also edited *in* CEDIN/Société tchèque pour le droit international, E. Decaux and A. Pellet eds., *Nationalité, minorités et succession d'Etats en Europe de l'Est*, Montchrestien, Paris, 1996, pp. 289-299.

- "Le droit", in Pascal BONIFACE ed., *La puissance internationale*, Dunod, Paris, 1994, pp. 145-156.

- "Note sur la Cour de conciliation et d'arbitrage au sein de la CSCE" *in* CEDIN - Fondation Marangopoulos pour les droits de l'homme, symposium of Athens, *La CSCE : dimension humaine et règlement des différends*, L.G.D.J., 1993, pp. 189-217.

- "Art du droit et 'science' des relations internationales" *in* Bertrand Badie and Alain Pellet eds., *Les relations internationales à l'épreuve de la science politique - Mélanges Marcel Merle*, Economica, 1993, pp.353-369.

- "L'activité de la Commission d'arbitrage de la Conférence européenne pour la paix en Yougoslavie", *Annuaire français de droit international*, 1992, pp. 200-238 et 1993, pp. 286-303.

- "The Normative Dilemma - Will and Consent in International Law", Report to the Canberra symposium, 1990, *Australian Yearbook of International Law*, vol. 12, 1992, pp. 22-53.

- "The Opinions of the Badinter Arbitration Committee - A Second Breath for the Self-Determination of Peoples", *European Journal of International Law*, 1992, pp. 178-185.

- "Role of the I.C.J. in a Changing U.N. Collective Security Context", *ASIL/NVIR Proceedings*, Nijhoff, Dordrecht, 1992, pp. 237-249.

- "The Destruction of Troy will not Take Place - There is but one Criterion Applicable in the Law of Belligerent Occupation : Respect for the Sovereign Rights of the Occupied People", International Commission of Jurists - Al Haq, Emma Playfair ed., *The Administration of Occupied Territories : The West Bank* (Jerusalem Symposium, 1988), Clarendon Press, Oxford, 1992, pp. 169-204; aslo published in French in *Palestinian Yearbook of International Law* 1987 - 1988, pp. 169 - 204.

- "Contre la tyrannie de la ligne droite - Aspects de la formation des normes en droit international de l'économie et du développement", course of lectures at the International Law Institute of Thessalonica, 1988, *in Thesaurus Acroasium*, vol. XIX, 1992, pp. 287-355.

- "Note sur la Commission d'arbitrage de la Conférence européenne pour la paix en Yougoslavie", *Annuaire français de droit international*, 1991, pp. 331-348.

- CEDIN, *Les aspects juridiques de la crise et de la guerre du Golfe*, Montchrestien, Paris, 1991, conclusions of the symposium, pp. 487-495.

- "Monetary Relations" *in* M. Bedjaoui ed., *International Law : Achievements and Prospects*; UNESCO, Nijhoff, Dordrecht, 1991, pp. 645-665; also published in French, Pedone, Paris, 1991, pp. 689-709.

- "Examen critique de la notion de droit au développement en droit international", U.N.O., Center for Human Rights, *Consultation globale sur la mise en oeuvre du droit au développement en tant que droit de l'homme*, 1990.

- "L'objet et la méthode en droit international - Y a-t-il une "méthode de Reims ?", Report to the 8th Reims symposium, Mai 1989, *Réalités du droit international contemporain, 8e rencontre de Reims*, CERI 1990, pp. 5-19.

- "Droit international et révolution - l'exemple du Cambodge" - Contribution to the Round Table, S.F.D.I., Symposium of Dijon, 1989, *in* S.F.D.I., *Révolution et droit international*, Pedone, 1990, pp. 275-279.

- "La mise en oeuvre des normes internationales des droits de l'homme", *in* C.E.D.I.N., *La France et des droits de l'Homme*, Montchrestien, Paris 1990, pp. 101-140.

- "Le glaive et la balance - Remarques sur le rôle de la Cour internationale de Justice en matière de maintien de la paix et de la sécurité internationales", *in* Yoram Dinstein ed., *International Law at a Time of Perplexity - Essays in Honour of Shabtai Rosenne*, Nijhoff, Dordrecht, 1989, pp. 539-566.

- "A New International Legal Order ? What Legal Tools for what Changes ?", Report to the Franco-British Symposium of London, *Aspects du droit international du développement* (January 1985), *in* Francis Snyder and Peter Slinn eds, *International Law of Development : Comparative Perspectives*, Professional Books, Abingdon, 1987, pp. 117-135; also published in *in* Yong Sang Cho ed., *Conflicts and Harmony in Modern Society*, Keimyung UP, Taegu, 1985, pp. 265-280.

- "Quelques problèmes institutionnels et juridiques posés par la coopération économique entre pays en développement au sein de la CNUCED", communication to the Rabat Symposium, *La coopération sud-est et l'avenir du Tiers monde*, *Revue juridique au Maroc*, 1986, pp. 123-134.

- "Le sage, le prince et le savant (A propos de "La politique juridique extérieure" de Guy de Lacharrière) ", *Journal du droit international* (*Clunet*), 1985, pp. 407-414.

- "Le droit au développement, un nouveau droit de l'homme ?" *in La formation des normes en droit international du développement*, collective work edited by Maurice Flory, CNRS-OPU 1985, pp. 71-85 (and conclusions of the symposium pp. 368-373).

- "La carrière des fonctionnaires internationaux" *in* S.F.D.I., symposium of Aix en Provence, *Les agents internationaux*, Pédone, 1985, pp.143-191.

- "Qui a peur du droit des peuples à disposer d'eux-mêmes ?", Critique socialiste, 1984, pp. 89-104.

- "The Functions of the Right to Development - A Right to Self-Realization", *Third World Legal Studies*, 1984, pp. 129-139.

- "Le bon droit et l'ivraie - Plaidoyer pour l'ivraie (Remarques sur quelques problèmes de méthode en droit international)", *Mélanges Charles Chaumont*, Pedone, 1984, pp. 465-493.

- "Légitime défense et agression - Le phénomène de libération nationale", 6th symposium of Reims, *Réalités du droit international contemporain - Discours juridique sur l'agression et réalité internationale*, CERI, Reims 1982, pp. 11-126.

- "Les voies de recours ouvertes aux fonctionnaires internationaux, recherche sur quelques problèmes d'actualité - L'exemple de la Commission de recours de l'O.C.D.E.", *Revue générale du droit international public*, 1981, n° 2, pp. 253-312, n° 4, pp. 657-792.

- "La reconnaissance par la France du droit de requête individuelle devant la Commission européenne des Droits de l'Homme" rapport au VIIe colloque de Besançon, 1980, *Revue du droit public et de la science politique*, 1981, pp. 69-103.

- "L'affaire Dumitrescu à l'UNESCO - Note sur l'indépendance des fonctionnaires internationaux", *Journal du droit international* (*Clunet*) 1979, pp. 570-103, n° 3.

- "L'article 53 de la Constitution de 1958 - Le rôle du Parlement dans la procédure d'entrée en vigueur des traités et accords internationaux" *in La Constitution de 1958*, edited by F.Luchaire and G.Conac, Economica 1979, pp. 671-709, updated 2nd ed. 1987, pp. 1005-1038.

- "Restructuration et démocratisation - l'exemple de la CNUCED et de l'ONUDI", report to the Algiers symposium, *Droit international et développement* (October 1976), O.P.U., Alger 1977, pp. 381-409)

- Corrected practical test : "Arrêt fictif de la C.I.J., dans l'affaire de Gibraltar - Les difficultés d'application du principe du droit des peuples à disposer d'eux-mêmes", *Revue de l'étudiant en droit*, Décembre 1976, pp. 74-80.

- "Budget et programmes aux Nations Unies, quelques tendances récentes", *Annuaire français de droit international*, 1976, pp. 242-282.

- Commentary of the decision of the Constitutional Court dated 15 January 1975, declaring the Parliamentary Act relating to the volontary interruption of pregnancy, in conformity with the Constitution, *Gazette du Palais*, 14-15 January 1976, p. 9.

- "La grève dans les services publics internationaux", *Revue générale du droit international public*, n° 4, 1975, pp. 932-971.

- "La ratification par la France de la Convention européenne des Droits de l'Homme", *Revue du droit public et de la science politique*, 1974, pp. 1319-1379.

- "La succession des organisations internationales et l'indépendance des fonctionnaires internationaux - A propos d'une décision de la Commission de recours du C.I.H.E.A.M.", *Annuaire français du droit international*, 1972, pp. 413-421.

- "Ventures between Multinational Corporations, Local Companies and Investors, and a Labor Union - Factory Machinery in World Markets" *in* Wolfang Friedmann and Jean-Pierre Béguin eds., *Joint International Business Ventures in Developing Countries*, Columbia University Press, New York and London 1971, pp. 167-184.

- Numerous reviews of books and articles in *Annuaire français de droit international* since 1969, *Journal du Droit International* (*Clunet*) since 1974 and *Politique étrangère* since 1989.

- Participation in numerous congresses and symposia in public international law, international development law and international relations.

- **Administrative Law - Notes on case law :**

- Council of State (Conseil d'Etat) (administrative court), Sect., 5 May 1972 - Société d'équipement de l'Indre and 21 July 1972, société "Entreprise Ossude" *J.C.P. (Semaine Juridique)*; 1973 n° 17481.

- Council of State, Sect., 19 January 1973, first case, Société d'exploitation électrique de la rivière du Sant ; second case, Minister of Industrial Development versus Le Vavasseur, *JCP (Semaine Juridique)*, 1971 n° 17629.

- Council of State, Ass., 2 November 1973, Société librairie Maspero (case of the "Tricontinental" journal), *Recueil Dalloz*, 1974 n° 432.

- Council of State, Ass., 18 January 1975, Da Silva and CFDT (case of the Marcellin-Fontanet circulars relating to immigration of foreign workers in France) *JCP (Semaine Juridique)*, 1976 n° 18235 et *Revue de l'étudiant en droit*, Avril 1977.

- Council of State, Ass., 13 February 1976, Association de sauvegarde du quartier Notre-Dame à Versailles, *Recueil Dalloz*, 1977, p.105.

-   **<u>Political Science :</u>**

-   *Une morale de la République - Pierre Mendes France et les institutions politiques*, Mémoire I.E.P. 1968, 246 ff.

-   *Pierre Mendes France et les événements de Mai et Juin 1968*. Mémoire D.E.S. de Sciences Politiques 1969, 108-LXXIII ff.

Exhibit 4

[February 20, 2013 Delgado email]

[New gTLD RG] Community objection - health

DELGADO, Rosa delgador at who.int
Wed Feb 20 16:47:17 UTC 2013

- Previous message: [New gTLD RG] Community objection - health
- Next message: [New gTLD RG] Google doc of preliminary draft of community objection statement on .health
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Thanks a LOT ++
Rosa                                    Contact Information Redacted
From: GEISSBUHLER Antoine
Sent: 20 February 2013 17:
To: newgtldrg at icann.org
Subject: Community objection - health

Dear Dev,

Please find attached an Overview file and the Health Community Objection Table, as requested.

Kind regards,

Antoine Geissbuhler
IMIA President

-------------- next part --------------
An HTML attachment was scrubbed...
URL: http://mm.icann.org/pipermail/newgtldrg/attachments/20130220/efe40a9f/attachment.html
```

- Previous message: [New gTLD RG] Community objection - health
- Next message: [New gTLD RG] Google doc of preliminary draft of community objection statement on .health
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Newgtldrg mailing list

Exhibit 5

[October 23, 2012 Delgado blog]

The Internet domain largest in its history. What happens in the health sector?

Top Level Domains (TLDs) and Health

This time we will talk about information technology and health sector, ie the top-level domains such as. Com,. Org. Info. Health,. Med. Doctor, etc.

The Internet is the main channel for the dissemination and access to information on education, health, commerce, industry, governance and civil society. In the health area, the Internet is consulted before the doctor, buy medicines online pharmacy without prescriptions or were screened for HIV or DNA through the network. On the other hand, many governments develop health strategies nationally as they are increasingly aware of the value of the Internet in public assistance and care.

The Internet Corporation for Assigned Names and Numbers (ICANN.org), is the authority that selects the managers of top-level domains, or TLDs (in English, Top Level Domains). The program of new generic TLDs (gTLDs) ICANN is now underway for the receipt of proposals and the selection of new gTLDs.

In 2000, seventy-five entities submitted proposals including the World Health Organization (WHO) to request the creation of a. 'Health' TLD for global health sector, which was not selected by ICANN but seven TLDs were approved (. aero,. museum,. coop,. info,. name, etc.). In 2004, one hundred entities submitted proposals and WHO did not show up. No entity requesting, 'health' or '. Healthcare' or any related TLD but ten were approved TLDs (. Post. Travel,. Xxx,. Mobi, etc.).

As explained in the preceding article, the May 30, 2012, ICANN received 1.930 proposals for the creation of new TLDs in any language and alphabet with immense opportunities for innovation. The dot-dot-brands and cities to be approved in 2013, which will be the first in the history of the Internet (. Google,. Pepsi,. Facebook. Paris,. Berlin,. NYC. Madrid, etc.).

Of which four proposals were for. 'Health' and sixteen health related names (ex.,. Health (in Chinese characters). Healthcare,. Med. Doctor. Hospital. Hiv,. Pharmacy, etc..) .

Today organizations such as WHO are trying to protect and prevent these TLDs such as. 'Health', which should be operated with the basic principles of public interest and not just commercial motivations - which is the case of the four applications of. health - are assigned by auction by ICANN.

WHO is doing lobbying with ICANN and its Government Advisory Council (GAC) to delay the selection of names. Health and allowing the global health community be consulted as this TLD should be created and operated. The aim is to mobilize the global community. 'Health' with stakeholders and Health Ministries compound, associations, health agencies, non-governmental organizations to consult who, how and who should operate the TLD - called . TLD health.

It is unacceptable that the. Health - to be sold to the private sector - can serve the indiscriminate sale of illegal drugs or alternative medicines or access to alternative clinics or hospitals that do not protect the confidentiality of patient's own public entities, etc. .

So WHO is beaten, when ICANN meetings and the last was that of Toronto conducted between 12-19 October 2012.

Other domains are sensitive to. Patagonia that has been requested by an American company in textiles but has the Patagonia brand in USA. The governments of Argentina and Chile are trying to avoid that this name is assigned by ICANN regional to a single company. Another is. Amazons that has been requested by the company Amazons who also holds the mark.

The Peruvian government should be alerted to the possibility that if a company has the mark or Sipan or Machupicchu Inca names or other assets, in next round of ICANN could also be assigned to individuals.

The author of this article is part of the delegation of WHO (www.who.int) for this item at ICANN. It was also the consultant of the European Broadcasting Union (www.ebu.ch) who presented the proposal to ICANN TLDs -. radio. eurovision, in May 2012.

In the next to give more news

Rosa Delgado

from Geneva

"The Internet domain largest in its history Why war around the Internet? "

No comments yet.

Leave a Reply

Name

Email

Website

Your
Comment

Submit Comment

7 + [ ] = Sixteen

LATEST ENTRIES

- Why war around the Internet?
- The Internet domain largest in its history. What happens in the health sector?
- The Internet domain largest in its history
- Hello world!

CATEGORIES

- Internet
- Internet and technology
- Uncategorized
- Technology

RECENT COMMENTS

- Anonymous on Hello world!

WOO THEMES

ATTACHMENT 3
(IO Reply)

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

ADDITIONAL WRITTEN STATEMENT

Filed by the Independent Objector

Limited Public Interest Objection

Disputed gTLD

gTLD Objector objects to

Name	.Hospital (Application ID: 1-1505-15195)
ICC Case No.	EXP/412/ICANN/29

EXPERT PANEL

Name	Prof. August Reinisch
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	Mr. Piotr Nowaczyk
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	Prof. Ike Ehiribe
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Identification of the Parties, their Representatives and related entities

Objector

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

Objector's Representative(s)

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

Email	Contact Information Redacted

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

Name	
Contact	
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Name	
Contact	
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Applicant

Name	Ruby Pike, LLC
Contact person	Daniel Schindler, Jon Nevett
Address	Contact Information Redacted
City, Country	
Telephone	

Email	Contact Information Redacted

Applicant's Representative(s)

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

Applicant's Contact Address

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

Procedure

On 12 March 2013, the Independent Objector electronically filed a Limited Public Interest objection to the Application of Ruby Pike LLC, for the gTLD string .Hospital (Application ID: 1-1505-15195). Electronic copies of the objection were transmitted to the Applicant and to ICANN on 13 March 2013.

On 29 March 2013, the DRSP informed the Independent Objector that it "has conducted the administrative review of the Objection in the above-referenced matter (Article 9 of the Procedure)" and that "the Objection is in compliance with Articles 5 – 8 of the Procedure and with the Rules."

On 15 April 2013, the DRSP further informed the Parties that ICANN had published its Dispute Announcement pursuant to Article 10(a) of the Procedure on 12 April 2013. It invited the Applicant to file a Response within 30 days of the transmission of this invitation (Article 11(b) of the Procedure).

On 15 May 2013, the Applicant electronically filed its Response to the Objection with Annexes. Electronic copies were transmitted to the Independent Objector and its representatives, as well as to ICANN.

On 19 June 2013, the DRSP informed the Parties that the Chairman of the Standing Committee appointed Prof. August Reinisch, Mr. Piotr Nowaczyk and Prof. Ike Ehiribe as Experts in the case and invited both Parties to make the required advance payment of costs for the Panel to be fully constituted. On 1 August 2013, the DRSP further informed the Parties of the receipt of the necessary advance payment and transferred the case file to the Expert Panel.

By E-Mail of 2 August 2013, the Independent Objector requested to file an additional written statement in order to address new issues that have been raised by Applicant's response. The Expert Panel granted this request. The Expert Panel fixed the time limit for the Independent Objector's additional written statement on 12 August 2013.

The present Additional Written Statement is filed accordingly.

Observations on the Response Submitted by the Applicant

Introduction

1.   In its at times rather aggressive Response the Applicant suggests in the first place that the Independent Objector (IO) is biased. Moreover, it is also suggested that his concerns about the applied-for .hospital string and, for that matter, about the applied-for .health gTLDs to which the IO also objected, somehow originate in a particular, private view of the IO on the status of *health* as a Human Right and on *hospitals* as one of the constitutive elements of this fundamental right to health (see, for example, the third paragraph on page 8 of the Response). Given the dismissive language used, the Applicant does not at all acknowledge that *health,* as a concept, is considered to be a Human Right, which status implies fundamental rights for citizens and specific obligations for States, and also for the private sector. However, it is precisely this status which led the IO to object to the applied-for introduction of .hospital as a new gTLD.

2.   Below, the IO will provide his observations on several of the issues discussed in the response, but before doing so, the IO wants to dispose of the Applicant's accusations that he or members of his legal team would somehow be biased.

The "Bias" Allegations are Groundless

3.   The Applicant calls into question the impartiality of the Independent Objector. Puzzlingly, it does not draw any procedural consequence from these allegations, but suggests that "the Panel should consider the Objection in light of his healthcare bias" (Response, p. 6). Even if the Applicant "do[es] not suggest [the IO] has engaged in any improper conduct" (*ibid*.), these unfounded allegations make it necessary for the IO to reaffirm his impartiality and independence.

4.   The IO has filed this objection (and all others objections) in accordance with Article 3.2.5 of the Guidebook stating that "the IO must be and remain independent and unaffiliated with any of the gTLD applicants". So he is. He has no relationship of any kind with any of the gTLD applicants in the present round. He is acting in no other interest but in the best interests of the public who use the global Internet. This is equally true for his legal representatives as well as for his assistant, specifically and unduly targeted by the Applicant (*ibid*., p. 6) and in the (very long) Declaration of Mr Nevett, annexed to the Response (*ibid*., Annex B, para. 18).

5. The Applicant reproaches the IO for having filed objections against medical-related gTLD applications (.Healthcare, .Hospital, .Medical, .Health), but not to all of them. It blames him for not having filed objections against many other strings that, in the Applicant's opinion, are "equally 'sensitive' as health".[1] The Applicant concludes that the IO has "some bias that favors medical interests" (*ibid*., p. 6). It attempts to "prove" this bias by an alleged professional relationship of the IO and the WHO, acknowledged in the IO's publicly available *curriculum vitae*[2].

6. Prof. Pellet's *c.v.* does record that he has served as counsel and advocate before the International Court of Justice in an advisory proceeding concerning a request of the WHO. However, the Applicant ignores the fact that, in that case, Prof. Pellet acted for the French Republic, not for the WHO[3]; this alone shows how artificial, and truly absurd, the Applicant's accusations are. In addition, Applicant's allegations concerning a relationship between the legal assistant of the IO, Mr. Boissise, and Ms Delgado, a consultant to WHO, on the sole basis of a non-existing LinkedIn connection "discovered" by Mr. Levett equally lack any substance. Applicant's evidence of bias is flimsy in the extreme and, in any event, it does not draw any conclusion from its (regrettable) allegations.

7. The simple position is that the IO is neither biased nor has favoured any particular interests, including medical interests. He has filed objections concerning gTLD applications for strings entirely unrelated to health and the healthcare sector, including .Amazon and its versions in languages others than English, .Charity and its other language versions, .Indians and .Patagonia[4]. Moreover, in the aim of ensuring transparency, the IO has explained on his public website why he decided not to file an objection against some "controversial" applications[5].

8. Applicant's allegation that the IO has not made objections to other equally "sensitive" strings also ignores the statutory limitations that the IO is subject to. According to Article 3.2.5 of the Applicant's Guidebook (hereafter the "Guidebook"): "In light of the public interest goal noted above, the IO shall not object to an application unless at least one comment in opposition to the application is made in the public sphere." Furthermore, he can only file

---

[1] It is important to recall that the IO is limited to filing objections on the ground of Limited Public Interest and Community grounds and cannot file an objection on the ground of violation of intellectual property right reason for example.

[2] http://www.alainpellet.eu/Documents/PELLET%20-%20cv%20long%20(ENG).pdf. See also Response, Annex B, Exhibit 3.

[3] See also the list of the delegations established by the International Court of Justice as part of the Verbatim Records, *CR 1995/22*, 30 October 1995, at pp. 5 and 6.

[4] http://www.independent-objector-newgtlds.org/english-version/the-independent-objector-s-objections/

[5] http://www.independent-objector-newgtlds.org/english-version/the-independent-objector-s-comments-on-controversial-applications/

Community objections or Limited Public Interest objections that are properly regulated, excluding String Confusion Objection or Legal Rights Objection.

9. Even if the Applicant does not say so expressly, it seems to reproach the IO for having especially targeted applications submitted by entities of Donuts, Applicant's ultimate parent. Indeed, the Applicant lists seven objections files by the IO against Donuts' related applications stating that "[t]he IO has filed relatively few objections overall, such that Donuts applications represent a significant proportion of them". In any case, the IO has filed objections against the applications that he considered to be contrary to the public's interests (Guidebook, Article 3.2.5.), which objections respond to the standards set out. He has justified his reasons in each of these objections, which are entirely indifferent to the identity of the Applicant. It may also be noted that Donuts has "applied for 307 new gTLDs"[6]. The IO's objections concern only 5 out of these 307 applied-for strings. The IO has filed comparable objections to applications for the same or identical strings submitted by entities unrelated with Donuts[7].

10. In conclusion, the allegations of bias lack any colourable basis, and are very much to be regretted.

The Objection is neither manifestly unfounded nor abusive

11. Clearly, the Expert Panel has not honoured the Applicant's request to dismiss the Objection in applying the 'quick look'-procedure. That the Objection is not manifestly unfounded, let alone abusive, has been upheld and confirmed by the Safeguard Advice issued by ICANN's Governmental Advisory Committee (GAC) on 11 April 2013 (**Annex 1**). In this document the GAC advises that extensive additional safeguards should be put in place for a whole range of TLDs. The .hospital TLD is included in this part of the advice (Annex 1, Category 1 of the GAC's advice). Also, the GAC advises to allow registration restrictions for particular strings – among them .hospital – which 'should be appropriate for the types of risks associated with the TLD' (Annex I, Category 2 of the GAC's advice). The GAC's Safeguard Advice confirms the concerns expressed by the IO in its Objection and the sensitivity of a new '.hospital' gTLD and demonstrates that those are not to be considered as abusive, nor as an harassment (page 9, first para. of the Response), as the Applicant would have it.

---

[6] Annex B, Declaration of Jonathon Nevett, founder and Executive Vice President of Donuts Inc., para. 5.- 8

[7] http://www.independent-objector-newgtlds.org/english-version/the-independent-objector-s-objections/

12. These concerns of the IO are, obviously, not diminished by the substance of the Response to the IO's Objection nor by the fact that the Applicant has reacted to the GAC advice in a very negative manner, while it has flatly rejected the special safeguards 6-8 advised by the GAC for strings that fall, among others, in the category 'health and fitness', among them '.hospital' (Donuts, Comment on GAC Advice, 23 May 2013, see page 12-13, http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf).

13. The recent Resolution adopted by the Sixty-sixth World Health Assembly on 27 May 2013 on "eHealth standardization and interoperability" also clearly confirms the IO's concerns raised in relation to this applied-for gTLD. In this Resolution, the World Health Assembly:

> "Emphasizing that health-related global top-level domain names in all languages, including ".health", should be operated in a way that protects public health, including by preventing the further development of illicit markets of medicines, medical devices and unauthorized health products and services;

> […]

> 2. Requests the Director- General […]:

> (6) to convey to the appropriate bodies, including the ICANN Governmental Advisory Committee and ICANN constituencies, the need for health-related global top-level domain names in all languages, including ".health", to be consistent with global public health objectives" (see **Annex** for the full text)

The IO is not acting outside of his mandate

14. The Applicant, through several avenues, endeavours to do away with the IO's Objection by arguing that it, one way or the other, is not in line with the concept of Limited Public Interest (LPI) Objections as foreseen in the Guidebook.

15. First, the Applicant assumes that the category of LPI Objections would be exclusively reserved for objections to the very *word*, or the *term* or the *simple expression* used for the applied-for new gTLD*.* This is, obviously, not the case. In this case the subject-matter of the Objection is not the word "healthcare" but rather its intended use and, in particular, its confiscation for purely commercial purposes which is contrary to general principles of

international law for morality and public order and likely to cause harmful consequences to the public.

16. The Guidebook, in its Attachment to Module 3 provides the following definition: "'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." (Article 2 (iii)). The Guidebook also states that the Expert Panel hearing a LPI Objection 'will conduct its analysis on the basis of the applied-for gTLD string itself. The panel may, if needed, use as additional context the intended purpose of the TLD as stated in the application' (Article 3.5.3., page 3-22). So, the question is not, or at least not only – and usually not primarily – whether the *word* is objectionable, but whether the proposed string and its intended operation may be objectionable from the perspective of 'general principles of international law for morality and public order'. The IO's position is of course not that the *word* "healthcare" would be objectionable *per se* but that the Application does not guarantee its use in full respect for these general principles.

17. More importantly, the Applicant pays no attention to the fact that the IO's Objection takes as its starting point that '"Health" is a crucial, existential need for each and every human being not seldom defining the difference between life and death' (paras 9 - 11 of the Objection). The Objection is explicitly based on the Universal Declaration of Human Rights and on the International Covenant on Economic, Social and Cultural Rights, both of which are listed in the – not exhaustive – list of instruments containing the general principles of international law for morality and public order (Guidebook, Article 3.5.3, pp. 3-21 and 3-22). So, contrary to what the Applicant suggests the challenged Objection is, as such, well within the standards defined in the Guidebook.

18. The Applicant further suggests that LPI Objections in general may only be raised in cases of incitement that are specifically – and as the Applicant would have it: exhaustively – listed in the Guidebook (violent lawless action, discrimination, sexual abuse of children) (see, in particular, Response, p. 9). The Applicant supports this suggestion by applying *eiusdem generis* as interpretation tool. Apparently the Applicant found this, online, in the 'Free Dictionary':

> " […] used to interpret loosely written statutes. Where a law lists specific classes of persons or things and then refers to them in general, the general statements only apply to the same kind of persons or things specifically listed. Example: if a law refers to automobiles, trucks, tractors, motorcycles *and* other

motor-powered vehicles, "vehicles" would not include airplanes, since the list was of land-based transportation." (http://legal-dictionary.thefreedictionary.com/Ejusdem+generis, italics added)

19. Quite apart from the fact that the Guidebook is not of the category of 'loosely written statutes', the IO notes that the fourth bullet point used in the summing-up in the Guidebook to which the Applicant refers is of a quite different nature than the previous three. Also the IO notes that in its paraphrasing the 'Free Dictionary', the Applicant conveniently left out the word '*and*', which in itself changes the applicability of the interpretation method and which is the more relevant since the listing of the three incitement-examples in the Guidebook does not use '*and*', but '*or*'. The latter is, obviously, in line with the non-exhaustive approach in the Guidebook, which approach is followed in the examples listed and also in the listing of sources from which the IO and, for that matter, the Expert Panels may draw when substantiating "generally accepted legal norms relating to morality and public order". Clearly, the consequences drawn by the Applicant from an *eiusdem generis*-approach, are ill-advised and they should be rejected.

20. Finally, the Applicant suggests that the IO infringes on its, and the public's, right to free speech. This is not correct. The IO started out with acknowledging the importance of freedom of expression as, also, a general principle of international law relating to morality and public order (Objection, para. 5). At the same time, freedom of expression is not free of any limits but "carries with it special duties and responsibilities" (Guidebook, Article 3.5.3, at p. 3-22). The concept of raising LPI Objections, and for that matter all objections envisaged by the Guidebook implies that these limits may lead to the rejection of certain applied-for strings.

The Applicant accepts no additional conditions

21. Clearly, the Applicant stresses all along that the applied-for string will be open to all consumers under whom all potential registrants. This inflexible position has been made clear by the Applicant in its Application, in its Response to the IO's Objection, in his Public Interest Commitment (PIC), and in its reaction to the GAC Safeguard Advice mentioned above. Although with respect to the latter, the language used by the Applicant seems to be nuanced on certain items, but with respect to its open-registration approach no nuance is to be discovered, while at crucial points in its reaction to the GAC advice refers to its PIC for its position (attached as **Annex 2**). The most striking part of the commitment laid down in its PIC is the very last sentence:

> "These PICs shall be subject to review by Registry Operator starting in January 2016, and *Registry Operator, in its sole discretion, may elect at that time to modify or discontinue any of the PICs herein* in the case of a substantial and compelling business need." (italics added)

This position is only reinforcing the IO to maintain his Request for Remedies as put forward in his Objection.

Remedies Requested

With respect to the remedies requested the Independent Objector maintains his position as set out in his Objection.

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

A copy of this Additional Written Statement is transmitted to the Applicant and its representatives on 12 August 2013 by e-mail to the following address: john@newgtlddisputes.com, don@newgtlddisputes.com, rubypike@donuts.co, secondary@donuts.co .

A copy of this Additional Written Statement is transmitted to ICANN on 12 August 2013 by e-mail to the following address: drfiling@icann.org

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

List and Provide description of any annex filed.

Annexes:
- GAC Advice Beijing Communique, April 2013
- Public Interest Commitments by Donuts
- Sixty-Sixth World Health Assembly, Resolution WHA66.24, eHealth standardization and interoperability, 27 May 2013 (http://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_R24-en.pdf)

Date: 12 August 2013

Signature: _____

[Governmental Advisory Committee](#)

Beijing, People's Republic of China – 11 April 2013

GAC Communiqué – Beijing, People's Republic of China[1]

I.   Introduction

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Beijing during the week of 4 April 2013. Sixty-one (61) GAC Members participated in the meetings and e**i**ght (8) Observers. The GAC expresses warm thanks to the local hosts China Internet Network Information Center (CNNIC), China Organizational Name Administration Center (CONAC), and Internet Society of China for their support.

II.   Internal Matters

1.   New Members and Observers

The GAC welcomes Belarus, Cape Verde, Côte d'Ivoire, Lebanon, and the Republic of the Marshall Islands to the Committee as members, and The World Meteorological Organisation as an Observer.

2.   GAC Secretariat

Following a request for proposals, the GAC received presentations from two organizations and agreed that one such candidate should be providing secretariat services to the GAC, with the aim of becoming operational as soon as possible. Negotiations with such organization will start immediately after the Beijing meeting.

---

[1] To access previous GAC advice, whether on the same or other topics, past GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Recent+Meetings and older GAC communiqués are available at: https://gacweb.icann.org/display/gacweb/GAC+Meetings+Archive.

3. **GAC Leadership**

   The GAC warmly thanks the outgoing Vice-Chairs, Kenya, Singapore, and Sweden and welcomes the incoming Vice-Chairs, Australia, Switzerland and Trinidad & Tobago.

III. Inter-constituencies Activities

1. **Meeting with the Accountability and Transparency Review Team 2 (ATRT 2)**

   The GAC met with the ATRT 2 and received an update on the current activities of the ATRT 2. The exchange served as an information gathering session for the ATRT 2 in order to hear GAC member views on the Review Team processes and areas of interest for governments. The GAC provided input on governmental processes and the challenges and successes that arose during the first round of reviews, and implementation of the GAC related recommendations of the first Accountability and Transparency Review Team.

2. **Board/GAC Recommendation Implementation Working Group (BGRI-WG)**

   The Board–GAC Recommendation Implementation Working Group (BGRI–WG) met to discuss further developments on ATRT1 recommendations relating to the GAC, namely recommendations 11 and 12. In the context of Recommendation 11, the GAC and the Board have concluded the discussion and agreed on the details of the consultation process mandated per ICANN Bylaws, should the Board decide not to follow a GAC advice. With respect to Recommendation 12, on GAC Early Engagement, the BGRI-WG had a good exchange with the GNSO on mechanisms for the GAC to be early informed and provide early input to the GNSO PDP. The BGRI–WG intends to continue this discussion intersessionally and at its next meeting in Durban.

3. **Brand Registry Group**

   The GAC met with the Brand Registry Group and received information on its origins, values and missions.

4. **Law Enforcement**

   The GAC met with law enforcement representatives and received an update from Europol on the Registrar Accreditation Agreement (RAA).

   ***

The GAC warmly thanks the Accountability and Transparency Review Team 2, the Brand Registry Group, Law Enforcement, and the ICANN Board who jointly met with the GAC as well

as all those among the ICANN community who have contributed to the dialogue with the GAC in Beijing.

IV. GAC Advice to the ICANN Board[2]

1. **New gTLDs**

a. **GAC Objections to Specific Applications**

i.   **The GAC Advises the ICANN Board that:**

i.   The GAC has reached consensus on GAC Objection Advice according to Module 3.1 part I of the Applicant Guidebook on the following applications:[3].

1. The application for .africa (Application number 1-1165-42560)

2. The application for .gcc (application number: 1-1936-2101)

ii. With regard to Module 3.1 part II of the Applicant Guidebook[4]:

1. The GAC recognizes that Religious terms are sensitive issues. Some GAC members have raised sensitivities on the applications that relate to Islamic terms, specifically .islam and .halal. The GAC members concerned have noted that the applications for .islam and .halal lack community involvement and support. It is the view of these GAC members that these applications should not proceed.

b. **Safeguard Advice for New gTLDs**

To reinforce existing processes for raising and addressing concerns the GAC is providing safeguard advice to apply to broad categories of strings (see Annex I).

c. **Strings for Further GAC Consideration**

In addition to this safeguard advice, that GAC has identified certain gTLD strings where further GAC consideration may be warranted, including at the GAC meetings to be held in Durban.

i.   Consequently, **the GAC advises the ICANN Board** to: not proceed beyond Initial Evaluation with the following strings : .shenzhen (IDN in Chinese), .persiangulf, .guangzhou (IDN in Chinese), .amazon (and IDNs in Japanese and Chinese), .patagonia, .date, .spa, . yun, .thai, .zulu, .wine, .vin

---

[2] To track the history and progress of GAC Advice to the Board, please visit the GAC Advice Online Register available at: https://gacweb.icann.org/display/gacweb/GAC+Recent+Meetings
[3] Module 3.1: "The GAC advises ICANN that it is the consensus of the GAC that a particular application should not proceed. This will create a strong presumption for the ICANN Board that the application should not be approved.
[4] Module 3.1: "The GAC advises ICANN that there are concerns about a particular application "dot-example." The ICANN Board is expected to enter into dialogue with the GAC to understand the scope of concerns. The ICANN Board is also expected to provide a rationale for its decision.

d. The GAC requests:

    i.   a written briefing about the ability of an applicant to change the string applied for in order to address concerns raised by a GAC Member and to identify a mutually acceptable solution.

e. Community Support for Applications

The GAC advises the Board:

    i.   that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information.

f. Singular and plural versions of the same string as a TLD

The GAC believes that singular and plural versions of the string as a TLD could lead to potential consumer confusion.

Therefore **the GAC advises the ICANN Board to:**

    i.   Reconsider its decision to allow singular and plural versions of the same strings.

g. Protections for Intergovernmental Organisations

The GAC stresses that the IGOs perform an important global public mission with public funds, they are the creations of government under international law, and their names and acronyms warrant special protection in an expanded DNS. Such protection, which the GAC has previously advised, should be a priority.

This recognizes that IGOs are in an objectively different category to other rights holders, warranting special protection by ICANN in the DNS, while also preserving sufficient flexibility for workable implementation.

The GAC is mindful of outstanding implementation issues and commits to actively working with IGOs, the Board, and ICANN Staff to find a workable and timely way forward.

Pending the resolution of these implementation issues, the **GAC reiterates its advice to the ICANN Board that:**

    i.   appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch.

2. **Registrar Accreditation Agreement (RAA)**

Consistent with previous communications to the ICANN Board

a. **the GAC advises the ICANN Board that:**

   i. the 2013 Registrar Accreditation Agreement should be finalized before any new gTLD contracts are approved.

The GAC also strongly supports the amendment to the new gTLD registry agreement that would require new gTLD registry operators to use only those registrars that have signed the 2013 RAA.

The GAC appreciates the improvements to the RAA that incorporate the 2009 GAC-Law Enforcement Recommendations.

The GAC is also pleased with the progress on providing verification and improving accuracy of registrant data and supports continuing efforts to identify preventative mechanisms that help deter criminal or other illegal activity. Furthermore the GAC urges all stakeholders to accelerate the implementation of accreditation programs for privacy and proxy services for WHOIS.

3. **WHOIS**

The GAC urges the ICANN Board to:

   a. ensure that the GAC Principles Regarding gTLD WHOIS Services, approved in 2007, are duly taken into account by the recently established Directory Services Expert Working Group.

The GAC stands ready to respond to any questions with regard to the GAC Principles.

The GAC also expects its views to be incorporated into whatever subsequent policy development process might be initiated once the Expert Working Group concludes its efforts.

4. **International Olympic Committee and Red Cross /Red Crescent**

Consistent with its previous communications, **the GAC advises the ICANN Board to:**

   a. amend the provisions in the new gTLD Registry Agreement pertaining to the IOC/RCRC names to confirm that the protections will be made permanent prior to the delegation of any new gTLDs.

5. **Public Interest Commitments Specifications**

The GAC requests:

      b.   more information on the Public Interest Commitments Specifications on the basis of the questions listed in annex II.

V. Next Meeting

The GAC will meet during the period of the 47th ICANN meeting in Durban, South Africa.

ANNEX I

Safeguards on New gTLDs

The GAC considers that Safeguards should apply to broad categories of strings. For clarity, this means any application for a relevant string in the current or future rounds, in all languages applied for**.**

The GAC advises the Board that all safeguards highlighted in this document as well as any other safeguard requested by the ICANN Board and/or implemented by the new gTLD registry and registrars should:

- be implemented in a manner that is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights.
- respect all substantive and procedural laws under the applicable jurisdictions.
- be operated in an open manner consistent with general principles of openness and non-discrimination.

Safeguards Applicable to all New gTLDs

The GAC Advises that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

1. **WHOIS verification and checks** —Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

2. **Mitigating abusive activity**—Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

3. **Security checks**— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

4. **Documentation**—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

5. **Making and Handling Complaints** – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

6. **Consequences** – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

The following safeguards are intended to apply to particular categories of new gTLDs as detailed below.

Category 1

Consumer Protection, Sensitive Strings, and Regulated Markets:

The GAC Advises the ICANN Board:

-   Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. The following safeguards should apply to strings that are related to these sectors:

    1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.
    2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.
    3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.
    4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

In the current round the GAC has identified the following non-exhaustive list of strings that the above safeguards should apply to:

- **Children:**
  - .kid, .kids, .kinder, .game, .games, .juegos, .play, .school, .schule, .toys
- **Environmental:**
  - .earth, .eco, .green, .bio, .organic
- **Health and Fitness:**
  - .care, .diet, .fit, .fitness, .health, .healthcare, .heart, .hiv, .hospital,, .med, .medical, .organic, .pharmacy, .rehab, .surgery, .clinic, .healthy (IDN Chinese equivalent), .dental, .dentist .doctor, .dds, .physio
- **Financial:**
  - capital, . cash, .cashbackbonus, .broker, .brokers, .claims, .exchange, .finance, .financial, .fianancialaid, .forex, .fund, .investments, .lease, .loan, .loans, .market, . markets, .money, .pay, .payu, .retirement, .save, .trading, .autoinsurance, .bank, .banque, .carinsurance, .credit, .creditcard, .creditunion,.insurance, .insure, ira, .lifeinsurance, .mortgage, .mutualfunds, .mutuelle, .netbank, .reit, .tax, .travelersinsurance, .vermogensberater, .vermogensberatung and .vesicherung.
- **Gambling:**
  - .bet, .bingo, .lotto, .poker, and .spreadbetting, .casino
- **Charity:**
  - .care, .gives, .giving, .charity (and IDN Chinese equivalent)
- **Education:**
  - degree, .mba, .university
- **Intellectual Property**
  - .audio, .book (and IDN equivalent), .broadway, .film, .game, .games, .juegos, .movie, .music, .software, .song, .tunes, .fashion (and IDN equivalent), .video, .app, .art, .author, .band, .beats, .cloud (and IDN equivalent), .data, .design, .digital, .download, .entertainment, .fan, .fans, .free, .gratis, .discount, .sale, .hiphop, .media, .news, .online, .pictures, .radio, .rip, .show, .theater, .theatre, .tour, .tours, .tvs, .video, .zip
- **Professional Services:**
  - .abogado, .accountant, .accountants, .architect, .associates, .attorney, .broker, .brokers, .cpa, .doctor, .dentist, .dds, .engineer, .lawyer, .legal, .realtor, .realty, .vet
- **Corporate Identifiers:**
  - .corp, .gmbh, .inc, .limited, .llc, .llp, .ltda, .ltd, .sarl, .srl, .sal
- **Generic Geographic Terms:**
  - .town, .city, .capital

- .reise, .reisen[5]
- .weather
- .engineering
- .law
- **Inherently Governmental Functions**
    o .army, .navy, .airforce
- In addition, applicants for the following strings should develop clear policies and processes to minimise the risk of cyber bullying/harassment
    o .fail, .gripe, .sucks, .wtf

The GAC further advises the Board:

1. In addition, some of the above strings may require further targeted safeguards, to address specific risks, and to bring registry policies in line with arrangements in place offline. In particular, a limited subset of the above strings are associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions, and the additional safeguards below should apply to some of the strings in those sectors:

    6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.
    7. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.

    8. The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

Category 2

Restricted Registration Policies

The GAC advises the ICANN Board:

1. **Restricted Access**
    o As an exception to the general rule that the gTLD domain name space is operated in an open manner registration may be restricted, in particular for strings mentioned under category 1

---

[5] Austria, Germany, and Switzerland support requirements for registry operators to develop registration policies that allow only travel-related entities to register domain names. Second Level Domains should have a connection to travel industries and/or its customers

above. In these cases, the registration restrictions should be appropriate for the types of risks associated with the TLD. The registry operator should administer access in these kinds of registries in a transparent way that does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage.

2. **Exclusive Access**
   - For strings representing generic terms, exclusive registry access should serve a public interest goal.

      - In the current round, the GAC has identified the following non-exhaustive list of strings that it considers to be generic terms, where the applicant is currently proposing to provide exclusive registry access

         - .antivirus, .app, .autoinsurance, .baby, .beauty, .blog, .book, .broker, .carinsurance, .cars, .cloud, .courses, .cpa, .cruise, .data, .dvr, .financialaid, .flowers, .food, .game, .grocery, .hair, .hotel, .hotels .insurance, .jewelry, .mail, .makeup, .map, .mobile, .motorcycles, .movie, .music, .news, .phone, .salon, .search, .shop, .show, .skin, .song, .store, .tennis, .theater, .theatre, .tires, .tunes, .video, .watches, .weather, .yachts, .クラウド [cloud], .ストア [store], .セール [sale], .ファッション [fashion], .家電 [consumer electronics], .手表 [watches], .書籍 [book], .珠宝 [jewelry], .通販 [online shopping], .食品 [food]

ANNEX II

List of questions related to Public Interest Commitments Specifications

1. Could a third party intervene or object if it thinks that a public interest commitment is not being followed? Will governments be able to raise those sorts of concerns on behalf of their constituents?

2. If an applicant does submit a public interest commitment and it is accepted are they able to later amend it? And if so, is there a process for that?

3. What are ICANN's intentions with regard to maximizing awareness by registry operators of their commitments?

4. Will there be requirements on the operators to maximize the visibility of these commitments so that stakeholders, including governments, can quickly determine what commitments were made?

5. How can we follow up a situation where an operator has not made any commitments? What is the process for amending that situation?

6. Are the commitments enforceable, especially later changes? Are they then going into any contract compliance?

7. How will ICANN decide whether to follow the sanctions recommended by the PIC DRP? Will there be clear and transparent criteria? Based on other Dispute Resolution Procedures what is the expected fee level?

8. If serious damage has been a result of the past registration policy, will there be measures to remediate the harm?

donuts

ICANN:

Attached please find the Public Interest Commitments (PICs) by the following applicants, subsidiaries of Donuts. We support the PIC process as a manageable and voluntary vehicle to make commitments in our applications binding, per the request of the ICANN Government Advisory Committee (GAC). These PICs do not conflict with the content of our applications.

With regard to #1 in the draft PIC Specification 11, it should be amended as redlined below to remove the open-ended right of the ICANN Board to approve a new form of the Registrar Accreditation Agreement at any point in the next 10 years with or without support of the other party to the agreement, and prohibiting us from providing registration services through any registrar that does not sign such agreement. As detailed in public comments, that is an over-reach and is not consistent with the multi-stakeholder model. With that said, we do not object to working with only those registrars that sign the 2013 RAA within a reasonable time period after it is approved by the ICANN Board, if it is in a form reasonably acceptable to the Registrar Stakeholder Group. We understand that the parties are close to achieving an approved agreement and we encourage them to do so forthwith.

We also provide these PICs cognizant that ICANN has not yet proposed any details of the PIC Dispute Resolution Policy (PICDRP) that would govern the enforcement of the PICs. We provide our PICs with the understanding that ICANN will provide an acceptable PICDRP.

Finally, we would like to reserve the right to supplement these PICs with additional commitments based on GAC and community feedback.

Jonathon Nevett
Co-Founder & EVP, Donuts Inc.

Applicant Name	Application No.	TLD	Applicant Name	Application No.	TLD
Knob Town, LLC	1-1340-40734	accountants	Binky Frostbite, LLC	1-1412-63109	creditcard
Spring Frostbite, LLC	1-1342-7920	architect	Tin Birch, LLC	1-1421-91857	dental
Victor North, LLC	1-1348-99321	attorney	Outer Lake, LLC	1-1422-97537	dentist
Holly Castle, LLC	1-1349-23181	audio	Brice Trail, LLC	1-1430-52453	doctor
Double Bloom, LLC	1-1361-60591	book	Outer Avenue, LLC	1-1452-20905	film
Corn Lake, LLC	1-1384-49318	charity	Cotton Cypress, LLC	1-1454-18725	finance
Black Corner, LLC	1-1390-429	claims	Over Keep, LLC	1-1465-93738	free
Goose Park, LLC	1-1392-58392	clinic	John Castle, LLC	1-1467-34522	fund
Trixy Canyon, LLC	1-1411-59458	cpa	Foggy Beach, LLC	1-1470-40168	games
Snow Shadow, LLC	1-1410-93823	credit	Pioneer Tigers, LLC	1-1481-2922	gratis

Goose Fest, LLC	1-1489-82287	**health**	June Woods, LLC	1-1544-18264	**loans**
Silver Glen, LLC	1-1492-32589	**healthcare**	Steel Hill, LLC	1-1561-23663	**medical**
Ruby Pike, LLC	1-1505-15195	**hospital**	Outer Gardens, LLC	1-1564-75367	**mortgage**
Auburn Park, LLC	1-1512-20834	**insurance**	New Frostbite, LLC	1-1570-42842	**movie**
Pioneer Willow, LLC	1-1516-617	**insure**	Victor Cross, LLC	1-1571-12951	**music**
Holly Glen, LLC	1-1521-75718	**investments**	Over Birch, LLC	1-1621-97265	**software**
Goose Gardens, LLC	1-1522-61364	**juegos**	Tin Avenue, LLC	1-1569-96051	**surgery**
Corn Dynamite, LLC	1-1523-55821	**law**	Storm Orchard, LLC	1-1562-9879	**tax**
Atomic Station, LLC	1-1531-96078	**lawyer**	Lone Tigers, LLC	1-1480-90854	**video**
Blue Falls, LLC	1-1536-79233	**legal**			

1.   Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on _____, 2013 (or any subsequent form of Registrar Accreditation Agreement approved by the ICANN Board of Directors) in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2.   □ Registry Operator will operate the registry for the TLD in compliance with all commitments, statements of intent and business plans stated in the following sections of Registry Operator's application to ICANN for the TLD, which commitments, statements of intent and business plans are hereby incorporated by reference into this Agreement. Registry Operator's obligations pursuant to this paragraph shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN ((posted at [url to be inserted when final procedure is adopted]), as it may be amended by ICANN from time to time, the "PICDRP"). Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

N/A

3.   ☑Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

Registry Operator agrees to the following Public Interest Commitments (PICs), which shall apply to this gTLD

1. Open registration
Second-level registrations in this gTLD will be open and available to lawful registrants. This gTLD represents a generic or dictionary term, and registry operator accordingly will operate it in an inclusive manner. Registry Operator will not limit registrant eligibility based on identity nor restrict availability of second-level names to only registrants whose identity is associated only with the most common usage of the term. Registry Operator will not disenfranchise lawful users who are associated with a minority usage of the term.

2. Geographic name protection

Pursuant to Specification 5 of this Registry Agreement, Registry Operator will transmit to registrars the list of geographic names prohibited from second-level registration. Registry Operator will periodically review this list to ensure it is identical to that maintained by ICANN. Should Registry Operator seek to release these reserved names, it will consult with ICANN's Governmental Advisory Committee and obtain any permissions necessary from ICANN for such release.

3. Rights Protection Mechanisms and Abuse Mitigation

> A.   Registry Operator commits to implementing and performing the following protections for this gTLD:

> 3.1   In order to help registrars and registrants identify inaccurate data in the Whois database, Registry Operator will audit Whois data for accuracy on a statistically significant basis.

3.2   Work with registrars and registrants to remediate inaccurate Whois data to help ensure a more accurate Whois database. Registry Operator reserves the right to cancel a domain name registration on the basis of inaccurate data, if necessary.

3.3   Establish and maintain a Domains Protected Marks List (DPML), a trademark protection service that allows rights holders to reserve registration of exact match trademark terms and terms that contain their trademarks across all gTLDs administered by Registry Operator under certain terms and conditions.

3.4   At no cost to trademark holders, establish and maintain a Claims Plus service, which is a notice protection mechanism that begins at the end of ICANN's mandated Trademark Claims period.

3.5   Bind registrants to terms of use that define and prohibit illegal or abusive activity.

3.6   Limit the use of proxy and privacy registration services in cases of malfeasance.

3.7   Consistent with the terms of this Registry Agreement, reserve the right to exclude from distribution any registrars with a history of non-compliance with the terms of the Registrar Accreditation Agreement.

3.8   Registry Operator will be properly resourced to perform these protections.

B.   Registry Operator also commits to the following protections for this gTLD:

1. Supplement the periodic audit of Whois data by more extensively reviewing and verifying data accuracy, and work to remediate inaccuracies.

2. Regularly monitor registered domain names for pharming, phishing, spam, botnets, copyright infringement, and other forms of abuse, and work to remediate any such activity. Registry Operator reserves the right to cancel registrations on the basis of abusive behavior, if necessary.

3. Require that registrars maintain a continually available point of contact capable of addressing problems involving abusive activity, and that registrars maintain the capability to remediate abuse or cancel a registration promptly, if necessary.

4. Anti-Abuse Policy

4.1   Registry Operator's Anti-Abuse Policy will be required under the Registry-Registrar Agreement and posted on the registry operator's web site.

4.2   Registry Operator will monitor the gTLD for abusive behavior and address it as soon as possible if detected.

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

4.3.1 to protect the integrity and stability of the registry;
4.3.2 to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
4.3.3 to comply with the terms of this Registry Agreement and the Registry Operator's Anti-Abuse Policy;
4.3.4 registrant fails to keep Whois information accurate and up-to-date;
4.3.5 domain name use violates the Registry Operator's acceptable use policies, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark; or
4.3.6 as needed during resolution of a dispute.

4.4   Abuse Point of Contact. Registry Operator will provide an abuse point of contact (APOC). This contact will be a role-based e-mail address posted on the Registry Operator's web site in the form such as "abuse123@registry.tld". This e-mail address will allow multiple staff members to monitor and address abuse reports. Registry Operator will further provide a convenient web form for complaints.

These PICs shall be subject to review by Registry Operator starting in January 2016, and Registry Operator, in its sole discretion, may elect at that time to modify or discontinue any of the PICs herein in the case of a substantial and compelling business need.

eHealth standardization and interoperability

The Sixty-sixth World Health Assembly,

Having considered the report by the Secretariat,[1]

Recalling resolution WHA58.28 on eHealth;

Recognizing that information and communication technologies have been incorporated in the Millennium Development Goals;

Recognizing that the Regional Committee for Africa adopted resolution AFR/RC60/R3 on eHealth in the African Region and that the 51st Directing Council of the Pan American Health Organization adopted resolution CD51.R5 on eHealth and has approved the related Strategy and Plan of Action; [2]

Recognizing that the secure, effective and timely transmission of personal data or population data across information systems requires adherence to standards on health data and related technology;

Recognizing that it is essential to make appropriate use of information and communication technologies in order to improve care, to increase the level of engagement of patients in their own care, as appropriate, to offer quality health services, to support sustainable financing of health care systems, and to promote universal access;

Recognizing that the lack of a seamless exchange of data within and between health information systems hinders care and leads to fragmentation of health information systems, and that improvement in this is essential to realize the full potential of information and communication technologies in health system strengthening;

Recognizing that, through standardized electronic data: health workers can gain access to fuller and more accurate information in electronic form on patients at the point of care; pharmacies can receive prescriptions electronically; laboratories can transmit test results electronically; imaging and diagnostic centres have access to high-quality digital images; researchers can carry out clinical trials and analyse data with greater speed and accuracy; public health authorities have access to electronic reports on vital events in a timely manner, and can implement public health measures based on the analysis of health data; and individuals can gain access to their personal medical information, which supports patient empowerment;

---

[1] Document A66/26.

[2] See document CD/51/13.

Recognizing that advances in medical health care, coupled with an exponential increase in the use of information and communication technologies in the health sector and other related fields, including the environment, have brought about a need to collect, store and process more data about patients and their environment in multiple computer and telecommunication systems and, therefore, ehealth standardization and interoperability should address standardization and interoperability issues related to hardware, systems, infrastructure, data and services;

Recognizing that the electronic collection, storage, processing and transmission of personal health data require adherence to the highest standards of data protection;

Recognizing that the electronic transmission of personal or population data using health information systems based on information and communication technologies requires adherence to standards in health data and technology in order to achieve a secure, timely and accurate exchange of data for health decision-making;

Emphasizing that scientific evaluation of the impact on health care outcomes of health information systems based on information and communication technologies is necessary to justify strong investment in such technologies for health;

Highlighting the need for national eHealth strategies to be developed and implemented, in order to provide the necessary context for the implementation of ehealth and health data standards, and in order that countries undertake regular, scientific evaluation;

Recognizing that it is essential to ensure secure online management of health data, given their sensitive nature, and to increase trust in eHealth tools and health services as a whole;

Emphasizing that health-related global top-level domain names in all languages, including ".health", should be operated in a way that protects public health, including by preventing the further development of illicit markets of medicines, medical devices and unauthorized health products and services;

1. URGES Member States:[1]

    (1) to consider, as appropriate, options to collaborate with relevant stakeholders, including national authorities, relevant ministries, health care providers, and academic institutions, in order to draw up a road map for implementation of ehealth and health data standards at national and subnational levels;

    (2) to consider developing, as appropriate, policies and legislative mechanisms linked to an overall national eHealth strategy, in order to ensure compliance in the adoption of ehealth and health data standards by the public and private sectors, as appropriate, and the donor community, as well as to ensure the privacy of personal clinical data;

    (3) to consider ways for ministries of health and public health authorities to work with their national representatives on the ICANN Governmental Advisory Committee in order to coordinate national positions towards the delegation, governance and operation of health-related global top-level domain names in all languages, including ".health", in the interest of public health;

---

[1] And, where applicable, regional economic integration organizations.

2.   REQUESTS the Director-General, within existing resources:

(1)   to provide support to Member States, as appropriate, in order to integrate the application of ehealth and health data standards and interoperability in their national eHealth strategies through a multistakeholder and multisectoral approach including national authorities, relevant ministries, relevant private sector parties, and academic institutions;

(2)   to provide support to Member States, as appropriate, in their promotion of the full implementation of ehealth and health data standards in all eHealth initiatives;

(3)   to provide guidance and technical support, as appropriate, to facilitate the coherent and reproducible evaluation of information and communication technologies in health interventions, including a database of measurable impacts and outcome indicators;

(4)   to promote full utilization of the network of WHO collaborating centres for health and medical informatics and eHealth in order to support Member States in related research, development and innovation in these fields;

(5)   to promote, in collaboration with relevant international standardization agencies, harmonization of eHealth standards;

(6)   to convey to the appropriate bodies, including the ICANN Governmental Advisory Committee and ICANN constituencies, the need for health-related global top-level domain names in all languages, including ".health", to be consistent with global public health objectives;

(7)   to continue working with the appropriate entities, including the ICANN Governmental Advisory Committee and ICANN constituencies as well as intergovernmental organizations, towards the protection of the names and acronyms of intergovernmental organizations, including WHO, in the Internet domain name system;

(8)   to develop a framework for assessing progress in implementing this resolution and report periodically, through the Executive Board, to the World Health Assembly, using that framework.

<div align="right">

Ninth plenary meeting, 27 May 2013
A66/VR/9

</div>

=   =   =

ATTACHMENT 4
(Ruby Pike Sur-Reply)

International Centre for Expertise   Centre international d'expertise

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

Prof. Alain Pellet,	ICC Case No. EXP/406/ICANN/29
Independent Objector (IO),	
-v-	In re Community Objection to: *<.HOSPITAL>* Application ID 1-1505-15195
Ruby Pike, LLC,	
Applicant/Respondent.	

Applicant's Response to
Objector's Additional Written Statement

INTRODUCTION

Objector's August 12, 2013 additional submission ("Reply") suffers from the same infirmity as the original Objection: it offers no *evidence* to meet Objector's significant burden to prove that the applied-for string <.HOSPITAL> – that is, the string itself – is "contrary to general principles of international law for morality and public order," as required for Limited Public Interest ("LPI") objections. AGB § 3.5.3. Indeed, Objector concedes he has no objection with the string itself. Reply ¶ 16.

Instead, Objector claims to bring a legitimate LPI Objection based on nothing more than speculation regarding matters *beyond the string* or its *intended use* as stated *in the Application*. AGB at 3-22. This effort must fail. ICANN did not appoint the IO to make new policy that he prefers to replace the policies agreed-upon by ICANN's multi-stakeholder process. The IO, at times, appears to have lost his mission, and has engaged conduct akin to prosecutorial overreach.

First, Objector has no evidentiary support for his assertions. Yet, "[e]vidence is appropriately required in all types of objection proceedings. Absent evidence, no objection should stand." http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf. "The objector bears the burden of *proof* in each case." AGB § 3.5 (emphasis added). The IO cannot escape his utter failure of proof in this case.

Second, the string is nothing more than the generic term "HOSPITAL," which can be used in a variety of perfectly legitimate ways, none of which being "contrary to…morality and

public order." Boundless examples could include animal hospitals (www.animalhospitals.com); or "hospitals" that fix fine jewelry (www.thejewelryhospital.com); automobiles (www.doylestonautohospital.com); Western cowboy boots (http://www.houstonshoehospital.com/about_us — est. 1906); major appliances (http://appliancehospital.com/); cellular telephones (https://www.facebook.com/pages/Cell-Phone-Hospital/194494470582521); personal computers (http://computer-hospital.com/); not to mention the popular television soap opera "General Hospital" (http://abc.go.com/shows/general-hospital) amongst a host of additional uses that people employ every day. While the Objection focuses solely upon a conventional treatment of the word "HOSPITAL," Applicant's view is that even widely-accepted meanings should not serve as a means of discriminating against other perfectly lawful, legitimate uses such as those described above.

Third, the Guidebook does not allow the IO or this Panel to look at anything past the string itself *other than* the *Application*. AGB § 3.5.3 at 3-22. Objector even quotes the controlling language, Reply ¶ 16, and then goes on to violate it. However, nothing in the Application suggests the <.HOSPITAL> domain would operate "contrary to general principles of international law for morality and public order." Rather, it states just the opposite – that Applicant will allow only lawful use of the domain. The inquiry ends there.

Fourth, even to the extent Objector strays outside the Guidebook standards, he fares no better. Applicant has explicitly recognized <.HOSPITAL> as a sensitive string. For this reason, in addition to the *fourteen protections* required by ICANN over and above what it currently imposes on existing gTLDs, and the *eight more* that Donuts has taken on voluntarily in *all* its applications, Applicant undertakes still *another four* measures. A <.HOSPITAL> gTLD run by Applicant will be safer than any gTLD the Internet has ever known, and a leader among *all* new gTLDs in that respect.

Finally, the April 11, 2013 Beijing communiqué issued by ICANN's Government Advisory Committee ("GAC") likewise provides no help to Objector. It expressly does *not* call for disallowance of a <.HOSPITAL> string, as the IO seeks. It seeks additional safeguards, most of which Applicant supports. Supp. Nevett Dec. ¶ 3. That support appears in the very link that the IO uses to characterize Applicant as a renegade actor. *See* http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf. Thus, the GAC advice has no relevance and provides no support to the IO's position here. If relevant at all, it favors Applicant and compels denial of the Objection. Applicant will have a contractual obligation to follow all GAC Advice adopted by ICANN, under penalty of losing the registry.

Such overreaching by the IO, coupled with the fact that he has devoted the bulk of his efforts to health-related domains in general and those applied for by Donuts in particular, has caused Applicant to question the Objector's true independence. Applicant has nothing further to add on that subject, and leaves it to the Panel to deny the Objection for its complete lack of merit, regardless of the IO's motives in bringing it.

ARGUMENT.

The Panel knows well that Objector bears the burden of proving each of the elements established by the Guidebook in order to prevail. AGB § 3.5. Objector must overcome the presumption of Applicant's entitlement to the domain, if qualified.[1] Specifically:

> There is a presumption generally in favor of granting new gTLDs to applicants who can satisfy the requirements for obtaining a gTLD –

---

[1] ICANN has certainly found Donuts amply qualified to operate a registry, as it has passed ICANN's Initial Evaluation (IE) on all 290 of its applications that ICANN has examined to date. Supp. Nevett Dec. ¶ 4 (**Annex 1** hereto).

and, hence, a corresponding burden upon a party that objects to the
gTLD to show why that gTLD should not be granted to the applicant.

http://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf.
Objector does not satisfy that burden.

Objector offers little more than the proposition – with which Applicant does not
disagree – that health is a fundamental human right, codified in significant source of
international law. Reply ¶ 17. Nowhere, however, does he present any *evidence* that a
<.HOSPITAL> *string*, or Donuts' plans for it *as stated in the Application*, would *violate* any
international legal protection pertaining to the subject. Nor can he, since nothing in the string
or the Application so demonstrates; rather, the opposite is true, as shown below.

A. *Objector Does Not Provide Evidence to Satisfy Guidebook Standards.*

Guidebook standards for LPI objections leave no room for doubt:

> An expert panel hearing a Limited Public Interest objection will
> consider whether the applied-for gTLD *string* is *contrary* to general
> principles of international law for morality and public order.

AGB § 3.5.3 at 3-20 (emphases added). Objector concedes that the string itself does not
satisfy that test. Reply ¶ 16. Nor does he provide any *evidence*, sufficient to meet his
burden of *proof*, of *violation* of international law *in any respect*.

Instead, the IO simply proclaims that Applicant's "confiscation" of the term
"HOSPITAL" for "commercial purposes" runs "contrary to general principles of international
law for morality and public order…." *Id.* ¶ 15 at 9-10. No precept of international law
supports this wholly conclusory and self-serving statement, and Objector certainly cites none.
Nor could he; otherwise, doctors, hospitals, pharmaceutical companies and other for-profit
HOSPITAL interests all will have somehow violated international law.

Nor does the IO find any indication of violation of international law in the Application.
The IO himself quotes from the portion of the Guidebook that explicitly provides:

> The panel will conduct its analysis on the basis of *the applied-for gTLD
> string itself*. The panel *may, if needed*, use as additional context the
> intended purpose of the TLD as stated *in the application*.

AGB § 3.5.3 at 3-22 (emphases added). Following the Guidebook, Objector's conclusion of
unlawfulness arising out of "purely commercial purposes," and unsubstantiated accusation of
Applicant's unwillingness to adopt certain "additional conditions" to safeguard a
<.HOSPITAL> domain, run headlong into evidence proving directly the opposite:

> This TLD is attractive and useful to end-users as it better facilitates
> search, self-expression, information sharing and the provision of
> *legitimate* goods and services.
>
> * * * * *
>
> In order to avoid harm to *legitimate* registrants, Donuts will not
> artificially deny access, … (*without legal cause*), to a TLD that
> represents a generic form of activity and expression.
>
> * * * * *

Restrictions on second level domain eligibility would prevent *law-abiding individuals and organizations* from participating in a space to which they are legitimately connected, and would inhibit the sort of positive innovation we intend to see in this TLD. .

* * * * *

By applying our array of protection mechanisms, Donuts will make this TLD a place for Internet users that is far safer than existing TLDs.

[Listing of 26 safeguards follows – 14 required by ICANN beyond those imposed on existing gTLDs, 8 more voluntarily adopted by Donuts to add additional protections to all of its applied-for gTLDs, and 4 additional protections directed specifically to <.HOSPITAL> as a "sensitive" domain.]

Resp. **Annex B**: Nevett Dec. ¶¶ 8-12, Ex. 1 ¶ 18(a) at 7-9 (emphases added). Objector at no time rebuts these or the many other statements throughout the Application that negate any conceivable LPI objection. Without such evidence, his Objection cannot succeed.

Instead, Objector speculates at to what hypothetical third parties *may* do with the domain at some later time. He argues for imposing pre-registration restrictions and advance verification for anyone seeking a <.HOSPITAL> TLD (*see* Reply ¶ 11), citing GAC "special safeguards 6 – 8" (Reply Ann. 1 at 10). Yet, the IO does not indicate how such policies should be implemented – *e.g.* in which countries to check or how to capture and evaluate such information from around the world. Nor does he justify why those who *review* or critique hospitals (such as journalists or even former or prospective patients), hospital suppliers, employees, contractors, aggregators, insurance companies and others that may use the gTLD in a lawful manner, should not also be allowed to register a <.HOSPITAL> domain.

Applicant supports an open gTLD and disagrees with the policy position taken by the IO. It believes in permitting the public to exercise its free expression unless such use violates the law, at which time the Applicant would take swift action. Objector fails to prove and cannot establish that Donuts' policy of not restricting speech *ex ante*, and taking action against any unlawful speech *ex post*, makes for a valid LPI objection. The IO's policy opinion simply does not discharge his burden or comport with the express standards of the Guidebook.

An example illustrates the point. Google and Amazon have applied for the <.TALK> domain. Under Objector's attenuated reasoning, since free speech is a "fundamental human right" and appears in the Universal Declaration of Human Rights, a would-be <.TALK> domain owner should impose a host of additional restrictions and pre-registration "eligibility requirements" in order to "guarantee" that "unworthy" speakers will not register second-level domains. Objector's argument would demand such "safeguards" solely on the grounds that "talk" can include obscenity, hate speech, defamation and other offensive material. While such *third-party material* could run afoul of international law standards for morality and public order, nothing in the string itself or its neutral operation does.

Donuts has applied for <.HOSPITAL>, not <.FREE-EBOLA-SAMPLES>, <.UNPROTECTED-SEX> or <MEDS-WITHOUT-PRESCRIPTIONS>. Nothing in its Application suggests that it will allow the sale of illegal drugs to children or any other activity that does not comport fully with all applicable laws. As such, neither the string itself nor its intended use as stated in the Application runs "contrary to general principles of international law for morality and public order."

Objector presents no evidence to overcome this plain reality. Without it, the Objection cannot stand.

A.   The GAC Beijing Communiqué Adds Nothing to the Objection.

Objector incorrectly asserts that his "concerns" have been "upheld and confirmed" by the GAC's Beijing communiqué. Reply ¶ 11. In it, the GAC identified over 100 strings, without reference to any particular applicant or application, that it believed generally should have "additional safeguards." The Panel can confirm this from the document itself, Reply Ann, 1, as opposed to Objector's characterization of it. *Ibid*. The Panel also can confirm that Applicant supports most of the GAC advice. *See* http://newgtlds.icann.org/sites/default/files/applicants/23may13/gac-advice-response-1-1336-51768-en.pdf ("The Board should accept most of the GAC advice and work toward implementation").

Objector asserts that the GAC's "concerns" align with his on the issue of registration restrictions. The GAC stated in its advice, however, that it recommends registration restrictions for only "some" of the listed strings. We do not yet know if <.HOSPITAL> is one of them. If it is, and the Board accepts the GAC advice, Applicant of course would abide by that decision. It is a *policy* decision, however, that should be made by the ICANN Board and not by the IO or this Panel. Current policy as expressed in the Guidebook does not proscribe the onerous restrictions for which the IO advocates, providing only for determination of whether a string or application itself would violate international law.

As such, the IO's position misapprehends the GAC's role, the Applicant's policy position, and the effect of its recommendations on the instant Objection. As noted, Applicant supports much of the Beijing GAC advice. However, it has no bearing on this objection proceeding and, in any event, does not extend nearly to the lengths that Objector would have this Panel go. If relevant at all, the Beijing communiqué, in the context of Guidebook standards, compels denial of the Objection.

The Guidebook contemplates that the GAC may provide "advice" to the ICANN Board to "address applications that are identified by governments to be problematic, e.g., that potentially violate national law or raise sensitivities." AGB § 3.1. "GAC Advice" may take one of three forms:

> (i) "that a particular application *should not proceed*," which "will create a *strong presumption* for the ICANN Board that the application should not be approved;"

> (ii) that the GAC has "*concerns*" about a particular string, as to which the ICANN board may "*enter into dialogue* with the GAC to understand the scope of concerns," then decide what to do about them and "provide a rationale for its decision;" or

> (iii) "that an application *should not proceed* unless remediated," which "will raise a *strong presumption* for the Board that the application should not proceed" absent such remediation.

Id. (emphases added) The GAC's Beijing comments regarding potentially "sensitive strings" such as <.HOSPITAL> take the second form, which does not call for rejection of the string or even create a "strong presumption" that such as a result should occur, whether outright or absent remediation. ICANN has no obligation to adopt all or any of the Beijing recommendations regarding the subject string. Such "advice," therefore, has no relevance whatsoever to the instant analysis.

Too, Objector overlooks the ultimate impact that the Beijing recommendations may have. ICANN in fact has accepted many of the protections suggested by the GAC at Beijing, and remains in "dialogue" with the GAC on the specific means of doing so with respect to

"Category 1" strings. *See* Supp. Nevett Dec. ¶ 2 and Ex. A (Annex 1 hereto). Whatever specific measures ICANN enacts will require implementation by Applicant in the form of a PIC, then embodied in a formal registry agreement by which Applicant must bind itself to undertake those measures under penalty of losing the registry – as Donuts has done in its registry agreement for another string. *Id*. ¶ 3 and Ex. B.

Ironically, then, the GAC advice to which Objector points as "evidence" of the potential for harm instead provides the precise process for ICANN to consider protections such as those for which Objector advocates. ICANN may require Applicant to do exactly what Objector claims it must do in order to avoid such harm. Because as Objector points out that ICANN already is considering such GAC advice in the appropriate process, the Panel need not concern itself with such policy discussion. Thus, the only "evidence" upon which Objector relies actually *defeats* the Objection.

CONCLUSION

Objector greatly overreaches. The Objection fails to meet Guidebook standards for LPI grounds. Rather, Objector argues outside the standards, or for his personal view of what they should be.

In so doing, he not only exceeds the bounds of the Guidebook; he infringes upon the free speech rights of Applicant and the general public – another core Guidebook principle. Aside from the atypical uses of the term "HOSPITAL" listed earlier, the simple fact is that an average consumer may want to discuss and critique certain "hospitals" that private companies or governments maintain without fear of censorship or reprisal. This seems completely lost on the Objector. He chooses instead to focus exclusively on vague, alarmist assertions about what a few miscreants may try to do if, in fact, Applicant is even awarded the TLD *and* fails to adhere to its explicit statements that it will only allow lawful conduct.

The Panel must decide within Guidebook constraints, based on the evidence before it and the burden of proof placed on the Objector. The Objection fails to satisfy the substantive LPI standards or his burden of proof. For these reasons, all as demonstrated more fully above and in its original Response, Applicant again respectfully urges the Panel to reject the ill-advised Objection.

DATED: August 20, 2013
Respectfully submitted,

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

By: _____/jmg/_____   By: _____/dcm/_____
    John M. Genga   Don C. Moody
john@newgtlddisputes.com   don@newgtlddisputes.com

Attorneys for Applicant/Respondent
RUBY PIKE, LLC

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

A copy of this Response is/was transmitted to the Objector on: August 20, 2013
by email to the following addresses: courriel@alainpellet.eu; avocet@bajer.fr;
mail@danielmueller.eu; phonvanderbiesen@vdbadvocaten.eu; and
swordsworth@essexcourt.net.

A copy of this Response is/was transmitted to ICANN on August 20, 2013 by e-mail to the
following addresses: DRfiling@icann.org.

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

Annex A – Supplemental Declaration of Jonathon Nevett

> *Exhibit A* – http://www.icann.org/en/news/announcements/announcement-2-03jul13-
> en.htm, 3 July 2013 New gTLD Program Committee Progress on Addressing GAC
> Beijing Advice on New gTLDs

> *Exhibit B* – Donuts Registry Agreement

Annex 1

[Supplemental Declaration of Jonathon Nevett]

DECLARATION OF JONATHON NEVETT

I, Jonathon Nevett, declare as follows:

1.   This declaration supplements my May 15, 2013 declaration in this matter, and supports applicant Ruby Pike, LLC's Response to Objector's Additional Written Statement herein. I make the statements herein from my own personal knowledge.

2.   I personally participated in responding to the communiqué issued by ICANN's Government Advisory Committee (GAC) at Beijing on April 11, 2013. As such, I also personally have followed ICANN's decisions concerning the recommendations in the GAC communiqué. Included herewith as Exhibit A is a true and correct copy of a publicly available July 3, 2013 report by the ICANN Board New gTLD Program Committee ("NGPC") regarding its "Progress on Addressing GAC Beijing Advice on New gTLDs." Starting at Item number 13 of the chart contained therein, the report reflects that the NGPC has accepted the GAC's six recommendations regarding safeguards for all gTLDs (Items 13-18), and remains in "dialogue" with the GAC regarding the eight measures proposed by the GAC with respect to the "Category 1" strings referenced in the communiqué, including <.HOSPITAL> (Items 19-26).

3.   Donuts supports much of the GAC Advice from Beijing. I am very familiar with what Donuts must do to implement any items of GAC Advice accepted by the ICANN Board. Donuts must make a "Public Interest Commitment" or "PIC" to adhere to each such recommendation, which then get embodied in a Registry Agreement with ICANN for the subject string. Donuts, in fact, already has done this for its first string. Included herewith as Exhibit B is a true and correct copy of its publicly available Registry Agreement for the Chinese-character gTLD for "GAMES." Specification 11 starting at page 87 of that Registry Agreement sets forth

1

Donuts' PICs for that string. Section 4.3(e) at page 11 of the Registry Agreement allows ICANN to terminate the agreement should Donuts breach the PICs set forth in Specification 11.

4.   As of the date of this declaration, Donuts has passed all 290 Initial Evaluations that ICANN has completed as to its applications.

I declare under penalty of perjury under the laws of the United States that based on my personal knowledge and belief the foregoing is true and correct and that this declaration was executed by me on August 20, 2013, in Rockville, Maryland, USA.

_____/jn/_____
Jonathon Nevett

Exhibit A

[3 July 2013 New gTLD Program Committee Progress on Addressing GAC Beijing Advice on New gTLDs]

Internet Corporation for Assigned Names and Numbers

Menu | Help | 🔍

NGPC Progress on Addressing GAC Beijing Advice on New gTLDs

3 July 2013

On 2 July 2013, the the ICANN Board New gTLD Program Committee (NGPC) had its seventh meeting to discuss the GAC Beijing advice on New gTLDs. The Committee took the following actions:

1. Initial Protections for IGO Protections

   In the Beijing Communiqué, the GAC reiterated previous advice that "appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch." In response to a number of issues raised by the Board, the GAC noted in the Beijing Communiqué that it is "mindful of outstanding implementation issues" and that it is committed to "actively working with IGOs, the Board, and ICANN Staff to find a workable and timely way forward. In a 6 June 2013 response letter to the GAC on the IGO GAC Advice, the ICANN Board Chairman proposed that a small number of NGPC members and ICANN staff begin a dialogue with the GAC on these issues

   At its 2 July 2013 meeting, the NGPC passed a resolution confirming that the New gTLD Registry Agreement will require operators to provide appropriate preventative initial protection for the IGO identifiers. These protections will remain in place while the GAC, NGPC, ICANN Staff and community continue to actively work through outstanding implementation issues. More specifically, registry operators will implement temporary protections for the IGO names and acronyms on the "IGO List dated 22/03/2013" until the first meeting of the NGPC following the ICANN 47 Meeting in Durban. The Resolution provides temporary protections for IGOs while respecting the ongoing work on implementation issues. The IGO List is attached to the Resolution as Annex 1.

   If the NGPC and GAC do not reach an agreement on outstanding implementation issues for protecting IGO names and acronyms by the first meeting of the NGPC following the ICANN 47 meeting in Durban, and subject to any matters that arise during the discussions, registry operators will be required to protect only the IGO names (and not the acronyms) identified on the GAC's IGO List.

2. Category 1 Advice

   In the Beijing Communiqué, the GAC proposed Category 1 safeguard advice, which includes recommended restrictions and consumer protections for sensitive strings and regulated markets. The Category 1 Safeguard Advice is divided into three main sections. The first section provides five (5) items of advice that apply to "strings that are linked to regulated or professional sectors." The Beijing Communiqué identified a list of strings to which this advice applies. The second

section provides three (3) additional pieces of advice that should apply to a limited subset of the strings noted in the GAC's list that are "associated with market sectors which have clear and/or or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions…." The third section includes an additional requirement for applicants for the following strings: .fail, .gripe, .sucks and .wtf.

On 23 April 2013, ICANN initiated a public comment forum to solicit input on how the NGPC should address GAC advice regarding safeguards applicable to broad categories of new gTLD strings http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm. The public comment forum closed on 4 June 2013. While many commenters voiced support for the Category 1 safeguard advice, many others submitting opposing comments. One overarching theme from the public comments was the need for additional clarity on the scope and intent of the Category 1 Safeguard Advice.

After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice.

3. New gTLD Registry Agreement

Finally, the NGPC considered the revised New gTLD Registry Agreement that will be entered into between ICANN and successful new gTLD applicants. The revised agreement is the result of several months of negotiations, formal community feedback (most recently during public comment forums initiated on 5 February 2013 on 29 April 2013), and meetings with various stakeholders and communities. The revisions include feedback from the ICANN community at the ICANN 46 Meeting on 7-11 April 2013 in Beijing as well as GAC advice issued in its Beijing Communiqué.

After considering the comments received from the community, the NGPC determined that the revised New gTLD Registry Agreement included significant improvements in response to the concerns raised by the community. The Committee also noted that in response to the GAC's Beijing Communiqué, revisions were made to Specification 11 to implement the non-Category 1 safeguard advice (i.e., safeguards applicable to all strings and Category 2 safeguards). The revisions to Specification 11 incorporate standardized language to address the safeguard advice. Applicant-specific PICs will be included on a case-by-case basis to the extent not superseded by or inconsistent with the standard PICs included to address the GAC's Beijing Communiqué.

The NGPC approved the form of the New gTLD Registry Agreement and authorized ICANN staff to take all necessary steps to implement it and to move forward with implementation of the New gTLD Program. The Agreement is attached to the Resolution as Annex 1; the complete Summary of Changes to the New gTLD Registry Agreement is attached to the Resolution as Annex 2; a redline of the current agreement as compared to the previous version dated 29 April 2013 is attached to the Resolution as Annex 3; and the Summary and Analysis of Public Comments is available at http://www.icann.org/en/news/public-comment/report-comments-base-agreement-01jul13-en.pdf [PDF, 338 KB].

All of the resolutions adopted at the 2 July 2013 NGPC meeting are posted at http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm. A table summarizing NGPC Consideration of the GAC's Beijing Advice appears below.

GAC Register #	Summary of GAC Advice	NGPC Position	NGPC Response
1. 2013-04-11-Obj-Africa (Communiqué §1.a.i.1)	The GAC Advises the ICANN Board that the GAC has reached consensus on GAC Objection Advice according to Module 3.1 part I of the Applicant Guidebook on the following application: .africa (Application number 1-1165-42560)	Accept	• Applicant was permitted to withdraw or seek relief according to ICANN's accountability mechanisms subject to the appropriate standing and procedural requirements. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
2. 2013-04-11-Obj-GCC (Communiqué §1.a.i.2)	The GAC Advises the ICANN Board that the GAC has reached consensus on GAC Objection Advice according to Module 3.1 part	Accept	• Applicant was permitted to withdraw or seek relief according to ICANN's accountability mechanisms subject to the appropriate standing and procedural requirements. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-

	I of the Applicant Guidebook on the following application: .gcc (application number: 1-1936-2101)		en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
3. 2103-04-11-Religious Terms (Communiqué §1.a.ii)	The GAC Advises the Board that with regard to Module 3.1 part II of the Applicant Guidebook, the GAC recognizes that Religious terms are sensitive issues. Some GAC members have raised sensitivities on the applications that relate to Islamic terms, specifically .islam and .halal. The GAC members concerned have noted that the applications for .islam and .halal lack community involvement and support. It is the view of these GAC members that these applications should not proceed.	Accept	• Pursuant to the requirements of Section 3.1.ii of the AGB, NGPC and GAC members will enter into a dialogue on this matter in Durban. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
4. 2013-04-11-gTLDStrings (Communiqué §1.c)	In addition to this safeguard advice, the GAC has identified certain gTLD strings where further GAC consideration may be warranted, including at the GAC meetings to be held in Durban. Consequently, the GAC advises the ICANN Board to not proceed beyond Initial Evaluation with the following strings : .shenzhen (IDN in Chinese), .persiangulf, .guangzhou (IDN in Chinese), .amazon (and IDNs in Japanese and Chinese), .patagonia, .date, .spa, .yun, .thai, .zulu, .wine, .vin	Accept	• ICANN has allowed evaluation and dispute resolution processes to go forward, but will not enter into registry agreements with applicants for the identified strings for now. • NGPC expects GAC to consider these applications further in Durban. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
5. Request for Written Briefing (Communiqué §1.d)	The GAC requests a written briefing about the ability of an applicant to change the string applied for in order to address concerns raised by a GAC Member and to identify a mutually acceptable solution.	Provided	Written briefing provided at https://gacweb.icann.org/download/attachments/28278832/NGPC%20Scorecard%20of%201As%20Regarding%20Non-%C2%ADSafeguard%20Advice%20in%20the%20GAC%20Beijing%20Communique%CC%81.pdf?version=1&modificationDate=1372384291000&api=v2 [PDF, 2.68 MB]
6. 2013-04-11-CommunitySupport (Communiqué §1.e)	The GAC advises the Board that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such	Accept	• Criterion 4 for the Community Priority Evaluation process takes into account "community support and/or opposition to the application" in determining whether to award priority to a community application in a contention set. • If a contention set is not resolved by the applicants or through a community priority evaluation then ICANN will utilize an auction as the objective method for resolving the contention.

	opinion should be duly taken into account, together with all other relevant information.		See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB].
7. 2013-04-11-PluralStrings (Communiqué §1.f)	The GAC believes that singular and plural versions of the string as a TLD could lead to potential consumer confusion. Therefore the GAC advises the Board to reconsider its decision to allow singular and plural versions of the same strings.	Accept	• After careful consideration of the issues, review of the comments raised by the community, the process documents of the expert review panels, and deliberations by the NGPC, the NGPC determined that no changes to the ABG are needed to address potential consumer confusion specifically resulting from allowing singular and plural versions of the same strings. • The NGPC considered several significant factors during its deliberations about whether to allow singular and plural version of the same strings. The NGPC had to balance the competing interests of each factor to arrive at a decision. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.d.
8. 2013-04-11-IGO (Communiqué §1.g)	GAC reiterates its advice to the ICANN Board that appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch.	Dialogue	• The New gTLD Registry Agreement will require operators to provide appropriate preventative initial protection for the IGO identifiers. These protections will remain in place while the GAC, NGPC, ICANN Staff and community continue to actively work through outstanding implementation issues. • If the NGPC and GAC do not reach an agreement on outstanding implementation issues for protecting IGO names and acronyms by the first meeting of the NGPC following the ICANN 47 meeting in Durban, and subject to any matters that arise during the discussions, registry operators will be required to protect only the IGO names (and not the acronyms) identified on the GAC's IGO List. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
9. 2013-04-11-RAA (Communiqué §2)	The GAC advises the ICANN Board that the 2013 Registrar Accreditation Agreement should be finalized before any new gTLD contracts are approved.	Accept	• The Board approved the 2013 RAA at its 27 June 2013 Meeting. • The 2013 RAA requires all new gTLD registries to only use 2013 RAA registrars. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
10. 2013-04-11-WHOIS (Communiqué §3)	The GAC urges the ICANN Board to ensure that the GAC Principles Regarding gTLD WHOIS Services, approved in 2007, are duly taken into account by the recently established Directory Services Expert Working Group.	Accept	• The GAC Principles have been shared with the Expert Working Group. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
			• The NGPC accepted the GAC advice. • The Registry Agreement includes protection for an indefinite duration for

11. 2013-04-11-IOCRC (Communiqué §4)	The GAC advises the ICANN Board to amend the provisions in the new gTLD Registry Agreement pertaining to the IOC/RCRC names to confirm that the protections will be made permanent prior to the delegation of any new gTLDs.	Accept	IOC/RCRC names. Specification 5 of this version of the Registry Agreement includes a list of names (provided by the IOC and RCRC Movement) that "shall be withheld from registration or allocated to Registry Operator at the second level within the TLD." • This protection was added pursuant to a NGPC resolution to maintain these protections "until such time as a policy is adopted that may require further action" (204.11.26.NG03). • The resolution recognized the GNSO's initiation of an expedited PDP. Until such time as the GNSO approves recommendations in the PDP and the Board adopts them, the NGPC's resolutions protecting IOC/RCRC names will remain in place. • Should the GNSO submit any recommendations on this topic, the NGPC will confer with the GAC prior to taking action on any such recommendations. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-04jun13-en.htm and http://www.icann.org/en/groups/board/documents/new-gtld-resolution-annex-1-04jun13-en.pdf [PDF, 564 KB]
12. 2013-04-11-PIC SPEC (Communiqué §5, Annex 2)	The GAC requests more information on the Public Interest Commitments Specifications on the basis of the questions listed in annex II.	Provided	NGPC responses to the Annex 2 questions available at https://gacweb.icann.org/display/GACADV/2013-04-11-PICSPEC
13. 2013-04-11-Safeguards 1 (Communiqué Annex 1, 1)	1. WHOIS verification and checks — Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.	Accept	• ICANN (instead of Registry Operators) will implement the GAC's advice that checks identifying registrations in a gTLD with deliberately false, inaccurate or incomplete WHOIS data be conducted at least twice a year. • ICANN will perform a periodic sampling of WHOIS data across registries in an effort to identify potentially inaccurate records. • ICANN will also maintain statistical reports that identify the number of inaccurate WHOIS records identified. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
14. 2013-04-11-Safeguards 2 (Communiqué Annex	2. Mitigating abusive activity— Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets,		• A provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) obligates Registry Operators to include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or

1, 2)	phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.	Accept	otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
15. 2013-04-11-Safeguards 3 (Communiqué Annex 1, 3)	3. Security checks— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.	Accept	• A provision in the New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) requires Registry Operators periodically to conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. • The provision also requires Registry Operators to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate. • Because there are multiple ways for a Registry Operator to implement the required security checks, ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality. • The language included in Paragraph 3 of the attached PIC Specification provides the general guidelines for what Registry Operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks. This will permit Registry Operators to enter into agreements as soon as possible, while allowing for a careful and fulsome consideration by the community on the implementation details. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
16. 2013-04-11-Safeguards 4 ((Communiqué Annex 1, 4)	4. Documentation—Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.	Accept	• As detailed in item 13 above, ICANN will maintain statistical reports that identify the number of inaccurate WHOIS records identified as part of the checks to identify registrations with deliberately false, inaccurate or incomplete WHOIS data. • As detailed in item 15 above, Registry Operators will be required to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. • Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.

17. 2013-04-11-Safeguards 5 ((Communiqué Annex 1, 5)	5. Making and Handling Complaints – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.	Accept	- Registry Operators are required to ensure that there is a mechanism for making complaints to the Registry Operator regarding malicious conduct in the TLD. - Section 4.1 of Specification 6 of the New gTLD Registry Agreement provides that, "Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquires related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details." - Section 2.8 of the New gTLD Registry Agreement provides that a, "Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD." - ICANN operates the WHOIS Data Problem Reports System <http://www.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form>, which is a mechanism for making complaints that WHOIS information is inaccurate. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
18. 2013-04-11-Safeguards 6 (Communiqué Annex 1, 6)	6. Consequences – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.	Accept	- Consequences for the demonstrated provision of false WHOIS information are set forth in Section 3.7.7.2 of the 2013 RAA <http://www.icann.org/en/resources/registrars/raa/proposed-agreement-22apr13-en.pdf> [PDF, 311 KB]: "A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration." - Paragraph 1 of the PIC Specification includes a requirement that Registry Operator will use only ICANN accredited registrars that are party to the 2013 RAA so that these consequences are contractually required. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b.
19. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 1)	1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.	Dialogue	- After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

20. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 2)	2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
21. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 3)	3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
22. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 4)	4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
23. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 5)	5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

24. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 6)	6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
25. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 7)	In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
26. 2013-04-11-Safeguards-Categories-1 (Communiqué Annex 1, Category 1, 8)	The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.	Dialogue	• After considering the community comments, the NGPC decided to begin a dialogue with the GAC during the ICANN Meeting in Durban to clarify the scope of the requirements provided in the Category 1 Safeguard Advice. The dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. Pending the dialogue with the GAC, staff will defer moving forward with the contracting process for applicants who have applied for TLD strings listed in the GAC's Category 1 Safeguard Advice. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.
27. 2013-04-11-Safeguards-Categories-2 (Communiqué Annex 1, Category 2, 1)	1. Restricted Access As an exception to the general rule that the gTLD domain name space is operated in an open manner registration may be restricted, in particular for strings mentioned under category 1 above. In these cases, the registration restrictions should be appropriate for the types of risks associated with the TLD. The registry operator should administer access in these kinds of registries in a transparent way that	Dialogue	• As noted above, the requested dialogue with the GAC on Category 1 will also include discussion of GAC's Category 2.1 Safeguard Advice regarding "Restricted Access" since that advice applies to the strings listed under Category 1. • See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-02jul13-en.htm.

	does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage.		
28. Safeguards-Categories-2 (Communiqué Annex 1, Category 2, 2)	**2. Exclusive Access** For strings representing generic terms, exclusive registry access should serve a public interest goal.	Accepted in part, dialogue on remainder	- For applicants seeking to impose exclusive registry access for "generic strings", the NGPC directed staff to defer moving forward with the contracting process for these applicants, pending a dialogue with the GAC. - The term "generic string" is defined to mean "a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others." - Exclusive registry access is defined as limiting registration of a generic string exclusively to a single person or entity and their affiliates. - For applicants not seeking to impose exclusive registry access, a provision in the in the New gTLD Registry Agreement requires TLDs to operate in a transparent manner consistent with general principles of openness and non-discrimination. - A PIC Specification also includes a provision to preclude registry operators from imposing eligibility criteria that limit registration of a generic string exclusively to a single person or entity and their "affiliates." - All applicants will be required to respond by a specified date indicating whether (a) the applicant is prepared to accept the proposed PIC Specification that precludes exclusive registry access or (b) the applicant is unwilling to accept the proposed PIC Specification because the applicant intends to implement exclusive registry access. - The NGPC will enter into a dialogue with the GAC to seek clarification on their advice with respect to exclusive registry access. - See http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.c.

RSS Feeds

RFPs

Litigation

Independent Review Process

Stay Connected

Your email address please.

News Alerts: ☐ HTML ☐ Plain Text
Newsletter: ☐ HTML ☐ Plain Text
Compliance
Newsletter: ☐ HTML ☐ Plain Text
Policy Update: ☐ HTML ☐ Plain Text

[Subscribe]

Follow us @icann   ICANN Blog

Videos   Community Wiki

Photos on Flickr   Planet ICANN

Facebook   RSS Feeds

Exhibit B

[Donuts Registry Agreement re Chinese-character "GAMES"]

REGISTRY AGREEMENT

This REGISTRY AGREEMENT (this "Agreement") is entered into as of 14 July 2013 (the "Effective Date") between Internet Corporation for Assigned Names and Numbers, a California nonprofit public benefit corporation ("ICANN"), and Spring Fields, LLC, a Delaware limited liability company ("Registry Operator").

ARTICLE 1.

DELEGATION AND OPERATION
OF TOP–LEVEL DOMAIN; REPRESENTATIONS AND WARRANTIES

1.1 **Domain and Designation**. The Top-Level Domain to which this Agreement applies is .游戏 (the "TLD"). Upon the Effective Date and until the earlier of the expiration of the Term (as defined in Section 4.1) or the termination of this Agreement pursuant to Article 4, ICANN designates Registry Operator as the registry operator for the TLD, subject to the requirements and necessary approvals for delegation of the TLD and entry into the root-zone.

1.2 **Technical Feasibility of String**. While ICANN has encouraged and will continue to encourage universal acceptance of all top-level domain strings across the Internet, certain top-level domain strings may encounter difficulty in acceptance by ISPs and webhosters and/or validation by web applications. Registry Operator shall be responsible for ensuring to its satisfaction the technical feasibility of the TLD string prior to entering into this Agreement.

1.3 **Representations and Warranties**.

(a)   Registry Operator represents and warrants to ICANN as follows:

(i)   all material information provided and statements made in the registry TLD application, and statements made in writing during the negotiation of this Agreement, were true and correct in all material respects at the time made, and such information or statements continue to be true and correct in all material respects as of the Effective Date except as otherwise previously disclosed in writing by Registry Operator to ICANN;

(ii)   Registry Operator is duly organized, validly existing and in good standing under the laws of the jurisdiction set forth in the preamble hereto, and Registry Operator has all requisite power and authority and has obtained all necessary approvals to enter into and duly execute and deliver this Agreement; and

(iii)   Registry Operator has delivered to ICANN a duly executed instrument that secures the funds required to perform registry functions for the TLD in the event of the termination or expiration of this Agreement (the "Continued Operations Instrument"), and such instrument is a binding

obligation of the parties thereto, enforceable against the parties thereto in accordance with its terms.

(b)   ICANN represents and warrants to Registry Operator that ICANN is a nonprofit public benefit corporation duly organized, validly existing and in good standing under the laws of the State of California, United States of America. ICANN has all requisite power and authority and has obtained all necessary corporate approvals to enter into and duly execute and deliver this Agreement.

ARTICLE 2.

COVENANTS OF REGISTRY OPERATOR

Registry Operator covenants and agrees with ICANN as follows:

2.1   Approved Services; Additional Services. Registry Operator shall be entitled to provide the Registry Services described in clauses (a) and (b) of the first paragraph of Section 2.1 in the Specification 6 attached hereto ("Specification 6") and such other Registry Services set forth on <u>Exhibit A</u> (collectively, the "Approved Services"). If Registry Operator desires to provide any Registry Service that is not an Approved Service or is a material modification to an Approved Service (each, an "Additional Service"), Registry Operator shall submit a request for approval of such Additional Service pursuant to the Registry Services Evaluation Policy at http://www.icann.org/en/registries/rsep/rsep.html, as such policy may be amended from time to time in accordance with the bylaws of ICANN (as amended from time to time, the "ICANN Bylaws") applicable to Consensus Policies (the "RSEP"). Registry Operator may offer Additional Services only with the written approval of ICANN, and, upon any such approval, such Additional Services shall be deemed Registry Services under this Agreement. In its reasonable discretion, ICANN may require an amendment to this Agreement reflecting the provision of any Additional Service which is approved pursuant to the RSEP, which amendment shall be in a form reasonably acceptable to the parties.

2.2   Compliance with Consensus Policies and Temporary Policies. Registry Operator shall comply with and implement all Consensus Policies and Temporary Policies found at <http://www.icann.org/general/consensus-policies.htm>, as of the Effective Date and as may in the future be developed and adopted in accordance with the ICANN Bylaws, provided such future Consensus Polices and Temporary Policies are adopted in accordance with the procedure and relate to those topics and subject to those limitations set forth in Specification 1 attached hereto ("Specification 1").

2.3   Data Escrow. Registry Operator shall comply with the registry data escrow procedures set forth in Specification 2 attached hereto ("Specification 2").

2.4   Monthly Reporting. Within twenty (20) calendar days following the end of each calendar month, Registry Operator shall deliver to ICANN reports in the format set forth in Specification 3 attached hereto ("Specification 3").

2.5   Publication of Registration Data. Registry Operator shall provide public access to registration data in accordance with Specification 4 attached hereto ("Specification 4").

2.6   Reserved Names. Except to the extent that ICANN otherwise expressly authorizes in writing, Registry Operator shall comply with the requirements set forth in Specification 5 attached hereto ("Specification 5"). Registry Operator may at any time establish or modify policies concerning Registry Operator's ability to reserve (i.e., withhold from registration or allocate to Registry Operator, but not register to third parties, delegate, use, activate in the DNS or otherwise make available) or block additional character strings within the TLD at its discretion. Except as specified in Specification 5, if Registry Operator is the registrant for any domain names in the registry TLD, such registrations must be through an ICANN accredited registrar, and will be considered Transactions (as defined in Section 6.1) for purposes of calculating the Registry-level transaction fee to be paid to ICANN by Registry Operator pursuant to Section 6.1.

2.7   Registry Interoperability and Continuity. Registry Operator shall comply with the Registry Interoperability and Continuity Specifications as set forth in Specification 6 attached hereto ("Specification 6").

2.8   Protection of Legal Rights of Third Parties. Registry Operator must specify, and comply with, the processes and procedures for launch of the TLD and initial registration-related and ongoing protection of the legal rights of third parties as set forth Specification 7 attached hereto ("Specification 7"). Registry Operator may, at its election, implement additional protections of the legal rights of third parties. Any changes or modifications to the process and procedures required by Specification 7 following the Effective Date must be approved in advance by ICANN in writing. Registry Operator must comply with all remedies imposed by ICANN pursuant to Section 2 of Specification 7, subject to Registry Operator's right to challenge such remedies as set forth in the applicable procedure described therein. Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.

2.9   Registrars.

(a)   All domain name registrations in the TLD must be registered through an ICANN accredited registrar; provided, that Registry Operator need not use a registrar if it registers names in its own name in order to withhold such names from delegation or use in accordance with Section 2.6. Subject to the requirements of Specification 11, Registry Operator must provide non-discriminatory access to Registry Services to all ICANN accredited registrars that enter into and are in compliance with the registry-registrar agreement for the TLD; provided that Registry Operator may establish non-discriminatory criteria for qualification to register names in the TLD that are reasonably related to the proper functioning of the TLD. Registry Operator must use a uniform non-discriminatory

agreement with all registrars authorized to register names in the TLD (the "Registry-Registrar Agreement"). Registry Operator may amend the Registry-Registrar Agreement from time to time; provided, however, that any material revisions thereto must be approved by ICANN before any such revisions become effective and binding on any registrar. Registry Operator will provide ICANN and all registrars authorized to register names in the TLD at least fifteen (15) calendar days written notice of any revisions to the Registry-Registrar Agreement before any such revisions become effective and binding on any registrar. During such period, ICANN will determine whether such proposed revisions are immaterial, potentially material or material in nature. If ICANN has not provided Registry Operator with notice of its determination within such fifteen (15) calendar-day period, ICANN shall be deemed to have determined that such proposed revisions are immaterial in nature. If ICANN determines, or is deemed to have determined under this Section 2.9(a), that such revisions are immaterial, then Registry Operator may adopt and implement such revisions. If ICANN determines such revisions are either material or potentially material, ICANN will thereafter follow its procedure regarding review and approval of changes to Registry-Registrar Agreements at <http://www.icann.org/en/resources/registries/rra-amendment-procedure>, and such revisions may not be adopted and implemented until approved by ICANN.

(b)   If Registry Operator (i) becomes an Affiliate or reseller of an ICANN accredited registrar, or (ii) subcontracts the provision of any Registry Services to an ICANN accredited registrar, registrar reseller or any of their respective Affiliates, then, in either such case of (i) or (ii) above, Registry Operator will give ICANN prompt notice of the contract, transaction or other arrangement that resulted in such affiliation, reseller relationship or subcontract, as applicable, including, if requested by ICANN, copies of any contract relating thereto; provided, that ICANN will treat such contract or related documents that are appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15 (except that ICANN may disclose such contract and related documents to relevant competition authorities). ICANN reserves the right, but not the obligation, to refer any such contract, related documents, transaction or other arrangement to relevant competition authorities in the event that ICANN determines that such contract, related documents, transaction or other arrangement might raise significant competition issues under applicable law. If feasible and appropriate under the circumstances, ICANN will give Registry Operator advance notice prior to making any such referral to a competition authority.

(c)   For the purposes of this Agreement: (i) "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, or in combination with one or more other persons or entities, controls, is controlled by, or is under common control with, the person or entity specified, and (ii) "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

2.10 Pricing for Registry Services.

(a) With respect to initial domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying or other programs which had the effect of reducing the price charged to registrars, unless such refunds, rebates, discounts, product tying or other programs are of a limited duration that is clearly and conspicuously disclosed to the registrar when offered) of no less than thirty (30) calendar days. Registry Operator shall offer registrars the option to obtain initial domain name registrations for periods of one (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(b) With respect to renewal of domain name registrations, Registry Operator shall provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the TLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying, Qualified Marketing Programs or other programs which had the effect of reducing the price charged to registrars) of no less than one hundred eighty (180) calendar days. Notwithstanding the foregoing sentence, with respect to renewal of domain name registrations: (i) Registry Operator need only provide thirty (30) calendar days notice of any price increase if the resulting price is less than or equal to (A) for the period beginning on the Effective Date and ending twelve (12) months following the Effective Date, the initial price charged for registrations in the TLD, or (B) for subsequent periods, a price for which Registry Operator provided a notice pursuant to the first sentence of this Section 2.10(b) within the twelve (12) month period preceding the effective date of the proposed price increase; and (ii) Registry Operator need not provide notice of any price increase for the imposition of the Variable Registry-Level Fee set forth in Section 6.3. Registry Operator shall offer registrars the option to obtain domain name registration renewals at the current price (i.e., the price in place prior to any noticed increase) for periods of one (1) to ten (10) years at the discretion of the registrar, but no greater than ten (10) years.

(c) In addition, Registry Operator must have uniform pricing for renewals of domain name registrations ("Renewal Pricing"). For the purposes of determining Renewal Pricing, the price for each domain registration renewal must be identical to the price of all other domain name registration renewals in place at the time of such renewal, and such price must take into account universal application of any refunds, rebates, discounts, product tying or other programs in place at the time of renewal. The foregoing requirements of this Section 2.10(c) shall not apply for (i) purposes of determining Renewal Pricing if the registrar has provided Registry Operator with documentation that demonstrates that the applicable registrant expressly agreed in its registration agreement with registrar to higher Renewal Pricing at the time of the initial registration of the domain name following clear and conspicuous disclosure of such Renewal Pricing to such registrant, and (ii) discounted Renewal Pricing pursuant to a Qualified Marketing Program (as defined below). The parties acknowledge that the purpose of this Section 2.10(c) is to prohibit abusive and/or discriminatory Renewal Pricing practices imposed by Registry

Operator without the written consent of the applicable registrant at the time of the initial registration of the domain and this Section 2.10(c) will be interpreted broadly to prohibit such practices. For purposes of this Section 2.10(c), a "Qualified Marketing Program" is a marketing program pursuant to which Registry Operator offers discounted Renewal Pricing, provided that each of the following criteria is satisfied: (i) the program and related discounts are offered for a period of time not to exceed one hundred eighty (180) calendar days (with consecutive substantially similar programs aggregated for purposes of determining the number of calendar days of the program), (ii) all ICANN accredited registrars are provided the same opportunity to qualify for such discounted Renewal Pricing; and (iii) the intent or effect of the program is not to exclude any particular class(es) of registrations (e.g., registrations held by large corporations) or increase the renewal price of any particular class(es) of registrations. Nothing in this Section 2.10(c) shall limit Registry Operator's obligations pursuant to Section 2.10(b).

(d)   Registry Operator shall provide public query-based DNS lookup service for the TLD (that is, operate the Registry TLD zone servers) at its sole expense.

2.11   Contractual and Operational Compliance Audits.

(a)   ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct, contractual compliance audits to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. Such audits shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit during regular business hours and in such a manner as to not unreasonably disrupt the operations of Registry Operator. As part of such audit and upon request by ICANN, Registry Operator shall timely provide all responsive documents, data and any other information reasonably necessary to demonstrate Registry Operator's compliance with this Agreement. Upon no less than ten (10) calendar days notice (unless otherwise agreed to by Registry Operator), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement. ICANN will treat any information obtained in connection with such audits that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of Registry Operator in accordance with Section 7.15.

(b)   Any audit conducted pursuant to Section 2.11(a) will be at ICANN's expense, unless (i) Registry Operator (A) controls, is controlled by, is under common control or is otherwise Affiliated with, any ICANN accredited registrar or registrar reseller or any of their respective Affiliates, or (B) has subcontracted the provision of Registry Services to an ICANN accredited registrar or registrar reseller or any of their respective Affiliates, and, in either case of (A) or (B) above, the audit relates to Registry Operator's compliance with Section 2.14, in which case Registry Operator shall reimburse ICANN for

all reasonable costs and expenses associated with the portion of the audit related to Registry Operator's compliance with Section 2.14, or (ii) the audit is related to a discrepancy in the fees paid by Registry Operator hereunder in excess of 5% in a given quarter to ICANN's detriment, in which case Registry Operator shall reimburse ICANN for all reasonable costs and expenses associated with the entirety of such audit. In either such case of (i) or (ii) above, such reimbursement will be paid together with the next Registry-Level Fee payment due following the date of transmittal of the cost statement for such audit.

(c)　　Notwithstanding Section 2.11(a), if Registry Operator is found not to be in compliance with its representations and warranties contained in Article 1 of this Agreement or its covenants contained in Article 2 of this Agreement in two consecutive audits conducted pursuant to this Section 2.11, ICANN may increase the number of such audits to one per calendar quarter.

(d)　　Registry Operator will give ICANN immediate notice of Registry Operator's knowledge of the commencement of any of the proceedings referenced in Section 4.3(d) or the occurrence of any of the matters specified in Section 4.3(f).

2.12　Continued Operations Instrument. Registry Operator shall comply with the terms and conditions relating to the Continued Operations Instrument set forth in Specification 8 attached hereto ("Specification 8").

2.13　Emergency Transition. Registry Operator agrees that, in the event that any of the emergency thresholds for registry functions set forth in Section 6 of Specification 10 is reached, ICANN may designate an emergency interim registry operator of the registry for the TLD (an "Emergency Operator") in accordance with ICANN's registry transition process (available at <http://www.icann.org/en/resources/registries/transition-processes>) (as the same may be amended from time to time, the "Registry Transition Process") until such time as Registry Operator has demonstrated to ICANN's reasonable satisfaction that it can resume operation of the registry for the TLD without the reoccurrence of such failure. Following such demonstration, Registry Operator may transition back into operation of the registry for the TLD pursuant to the procedures set out in the Registry Transition Process, provided that Registry Operator pays all reasonable costs incurred (i) by ICANN as a result of the designation of the Emergency Operator and (ii) by the Emergency Operator in connection with the operation of the registry for the TLD, which costs shall be documented in reasonable detail in records that shall be made available to Registry Operator. In the event ICANN designates an Emergency Operator pursuant to this Section 2.13 and the Registry Transition Process, Registry Operator shall provide ICANN or any such Emergency Operator with all data (including the data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by ICANN or such Emergency Operator. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event that an Emergency Operator is designated pursuant to this Section 2.13. In addition, in the

event of such failure, ICANN shall retain and may enforce its rights under the Continued Operations Instrument.

2.14 Registry Code of Conduct. In connection with the operation of the registry for the TLD, Registry Operator shall comply with the Registry Code of Conduct as set forth in Specification 9 attached hereto ("Specification 9").

2.15 Cooperation with Economic Studies. If ICANN initiates or commissions an economic study on the impact or functioning of new generic top-level domains on the Internet, the DNS or related matters, Registry Operator shall reasonably cooperate with such study, including by delivering to ICANN or its designee conducting such study all data related to the operation of the TLD reasonably necessary for the purposes of such study requested by ICANN or its designee, provided, that Registry Operator may withhold (a) any internal analyses or evaluations prepared by Registry Operator with respect to such data and (b) any data to the extent that the delivery of such data would be in violation of applicable law. Any data delivered to ICANN or its designee pursuant to this Section 2.15 that is appropriately marked as confidential (as required by Section 7.15) shall be treated as Confidential Information of Registry Operator in accordance with Section 7.15, provided that, if ICANN aggregates and makes anonymous such data, ICANN or its designee may disclose such data to any third party. Following completion of an economic study for which Registry Operator has provided data, ICANN will destroy all data provided by Registry Operator that has not been aggregated and made anonymous.

2.16 Registry Performance Specifications. Registry Performance Specifications for operation of the TLD will be as set forth in Specification 10 attached hereto ("Specification 10"). Registry Operator shall comply with such Performance Specifications and, for a period of at least one (1) year, shall keep technical and operational records sufficient to evidence compliance with such specifications for each calendar year during the Term.

2.17 Additional Public Interest Commitments. Registry Operator shall comply with the public interest commitments set forth in Specification 11 attached hereto ("Specification 11").

2.18 Personal Data. Registry Operator shall (i) notify each ICANN-accredited registrar that is a party to the registry-registrar agreement for the TLD of the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to Registry Operator by such registrar is collected and used under this Agreement or otherwise and the intended recipients (or categories of recipients) of such Personal Data, and (ii) require such registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. Registry Operator shall take reasonable steps to protect Personal Data collected from such registrar from loss, misuse, unauthorized disclosure, alteration or destruction. Registry Operator shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

ARTICLE 3.

COVENANTS OF ICANN

ICANN covenants and agrees with Registry Operator as follows:

3.1 **Open and Transparent**. Consistent with ICANN's expressed mission and core values, ICANN shall operate in an open and transparent manner.

3.2 **Equitable Treatment**. ICANN shall not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and shall not single out Registry Operator for disparate treatment unless justified by substantial and reasonable cause.

3.3 **TLD Nameservers**. ICANN will use commercially reasonable efforts to ensure that any changes to the TLD nameserver designations submitted to ICANN by Registry Operator (in a format and with required technical elements specified by ICANN at http://www.iana.org/domains/root/ will be implemented by ICANN within seven (7) calendar days or as promptly as feasible following technical verifications.

3.4 **Root-zone Information Publication.** ICANN's publication of root-zone contact information for the TLD will include Registry Operator and its administrative and technical contacts. Any request to modify the contact information for the Registry Operator must be made in the format specified from time to time by ICANN at http://www.iana.org/domains/root/.

3.5 **Authoritative Root Database**. To the extent that ICANN is authorized to set policy with regard to an authoritative root server system (the "Authoritative Root Server System"), ICANN shall use commercially reasonable efforts to (a) ensure that the authoritative root will point to the top-level domain nameservers designated by Registry Operator for the TLD, (b) maintain a stable, secure, and authoritative publicly available database of relevant information about the TLD, in accordance with ICANN publicly available policies and procedures, and (c) coordinate the Authoritative Root Server System so that it is operated and maintained in a stable and secure manner; provided, that ICANN shall not be in breach of this Agreement and ICANN shall have no liability in the event that any third party (including any governmental entity or internet service provider) blocks or restricts access to the TLD in any jurisdiction.

ARTICLE 4.

TERM AND TERMINATION

4.1 **Term**. The term of this Agreement will be ten (10) years from the Effective Date (as such term may be extended pursuant to Section 4.2, the "Term").

4.2 **Renewal**.

(a)   This Agreement will be renewed for successive periods of ten (10) years upon the expiration of the initial Term set forth in Section 4.1 and each successive Term, unless:

(i)   Following notice by ICANN to Registry Operator of a fundamental and material breach of Registry Operator's covenants set forth in Article 2 or breach of its payment obligations under Article 6 of this Agreement, which notice shall include with specificity the details of the alleged breach, and such breach has not been cured within thirty (30) calendar days of such notice, (A) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator has been in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (B) Registry Operator has failed to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction; or

(ii)   During the then current Term, Registry Operator shall have been found by an arbitrator (pursuant to Section 5.2 of this Agreement) or a court of competent jurisdiction on at least three (3) separate occasions to have been in (A) fundamental and material breach (whether or not cured) of Registry Operator's covenants set forth in Article 2 or (B) breach of its payment obligations under Article 6 of this Agreement.

(b)   Upon the occurrence of the events set forth in Section 4.2(a) (i) or (ii), the Agreement shall terminate at the expiration of the then-current Term.

4.3   Termination by ICANN.

(a)   ICANN may, upon notice to Registry Operator, terminate this Agreement if: (i) Registry Operator fails to cure (A) any fundamental and material breach of Registry Operator's representations and warranties set forth in Article 1 or covenants set forth in Article 2, or (B) any breach of Registry Operator's payment obligations set forth in Article 6 of this Agreement, each within thirty (30) calendar days after ICANN gives Registry Operator notice of such breach, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in fundamental and material breach of such covenant(s) or in breach of its payment obligations, and (iii) Registry Operator fails to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(b)   ICANN may, upon notice to Registry Operator, terminate this Agreement if Registry Operator fails to complete all testing and procedures (identified by ICANN in writing to Registry Operator prior to the date hereof) for delegation of the TLD into the root zone within twelve (12) months of the Effective Date. Registry Operator may

request an extension for up to additional twelve (12) months for delegation if it can demonstrate, to ICANN's reasonable satisfaction, that Registry Operator is working diligently and in good faith toward successfully completing the steps necessary for delegation of the TLD. Any fees paid by Registry Operator to ICANN prior to such termination date shall be retained by ICANN in full.

(c)   ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator fails to cure a material breach of Registry Operator's obligations set forth in Section 2.12 of this Agreement within thirty (30) calendar days of delivery of notice of such breach by ICANN, or if the Continued Operations Instrument is not in effect for greater than sixty (60) consecutive calendar days at any time following the Effective Date, (ii) an arbitrator or court of competent jurisdiction has finally determined that Registry Operator is in material breach of such covenant, and (iii) Registry Operator fails to cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(d)   ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator makes an assignment for the benefit of creditors or similar act, (ii) attachment, garnishment or similar proceedings are commenced against Registry Operator, which proceedings are a material threat to Registry Operator's ability to operate the registry for the TLD, and are not dismissed within sixty (60) calendar days of their commencement, (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registry Operator or maintains control over any of Registry Operator's property, (iv) execution is levied upon any material property of Registry Operator, (v) proceedings are instituted by or against Registry Operator under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within sixty (60) calendar days of their commencement, or (vi) Registry Operator files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101, et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations or the operation of the TLD.

(e)   ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement pursuant to Section 2 of Specification 7 or Sections 2 and 3 of Specification 11, subject to Registry Operator's right to challenge such termination as set forth in the applicable procedure described therein.

(f)   ICANN may, upon notice to Registry Operator, terminate this Agreement if (i) Registry Operator knowingly employs any officer who is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) calendar days of Registry Operator's knowledge of the foregoing, or (ii) any member of Registry Operator's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the

subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registry Operator's board of directors or similar governing body within thirty (30) calendar days of Registry Operator's knowledge of the foregoing.

(g)   ICANN may, upon thirty (30) calendar days' notice to Registry Operator, terminate this Agreement as specified in Section 7.5.

4.4   Termination by Registry Operator.

(a)   Registry Operator may terminate this Agreement upon notice to ICANN if (i) ICANN fails to cure any fundamental and material breach of ICANN's covenants set forth in Article 3, within thirty (30) calendar days after Registry Operator gives ICANN notice of such breach, which notice will include with specificity the details of the alleged breach, (ii) an arbitrator or court of competent jurisdiction has finally determined that ICANN is in fundamental and material breach of such covenants, and (iii) ICANN fails to comply with such determination and cure such breach within ten (10) calendar days or such other time period as may be determined by the arbitrator or court of competent jurisdiction.

(b)   Registry Operator may terminate this Agreement for any reason upon one hundred eighty (180) calendar day advance notice to ICANN.

4.5   Transition of Registry upon Termination of Agreement. Upon expiration of the Term pursuant to Section 4.1 or Section 4.2 or any termination of this Agreement pursuant to Section 4.3 or Section 4.4, Registry Operator shall provide ICANN or any successor registry operator that may be designated by ICANN for the TLD in accordance with this Section 4.5 with all data (including the data escrowed in accordance with Section 2.3) regarding operations of the registry for the TLD necessary to maintain operations and registry functions that may be reasonably requested by ICANN or such successor registry operator. After consultation with Registry Operator, ICANN shall determine whether or not to transition operation of the TLD to a successor registry operator in its sole discretion and in conformance with the Registry Transition Process; provided, however, that (i) ICANN will take into consideration any intellectual property rights of Registry Operator (as communicated to ICANN by Registry Operator) in determining whether to transition operation of the TLD to a successor registry operator and (ii) if Registry Operator demonstrates to ICANN's reasonable satisfaction that (A) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator or its Affiliates for their exclusive use, (B) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (C) transitioning operation of the TLD is not necessary to protect the public interest, then ICANN may not transition operation of the TLD to a successor registry operator upon the expiration or termination of this Agreement without the consent of Registry Operator (which shall not be unreasonably withheld, conditioned or delayed). For the avoidance of doubt, the foregoing sentence shall not prohibit ICANN from delegating the TLD pursuant to a future application process for the delegation of top-level domains, subject to any

processes and objection procedures instituted by ICANN in connection with such application process intended to protect the rights of third parties. Registry Operator agrees that ICANN may make any changes it deems necessary to the IANA database for DNS and WHOIS records with respect to the TLD in the event of a transition of the TLD pursuant to this Section 4.5. In addition, ICANN or its designee shall retain and may enforce its rights under the Continued Operations Instrument for the maintenance and operation of the TLD, regardless of the reason for termination or expiration of this Agreement.

4.6   Effect of Termination. Upon any expiration of the Term or termination of this Agreement, the obligations and rights of the parties hereto shall cease, provided that such expiration or termination of this Agreement shall not relieve the parties of any obligation or breach of this Agreement accruing prior to such expiration or termination, including, without limitation, all accrued payment obligations arising under Article 6. In addition, Article 5, Article 7, Section 2.12, Section 4.5, and this Section 4.6 shall survive the expiration or termination of this Agreement. For the avoidance of doubt, the rights of Registry Operator to operate the registry for the TLD shall immediately cease upon any expiration of the Term or termination of this Agreement.

ARTICLE 5.

DISPUTE RESOLUTION

5.1   Mediation. In the event of any dispute arising under or in connection with this Agreement, before either party may initiate arbitration pursuant to Section 5.2 below, ICANN and Registry Operator must attempt to resolve the dispute through mediation in accordance with the following terms and conditions:

(a)   A party shall submit a dispute to mediation by written notice to the other party. The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days of delivery of written notice pursuant to this Section 5.1, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 5.1(a).

(b)   The mediator shall conduct the mediation in accordance with the rules and procedures that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute. The mediation shall be treated as a settlement discussion and shall therefore be confidential and may not be used against

either party in any later proceeding relating to the dispute, including any arbitration pursuant to Section 5.2. The mediator may not testify for either party in any later proceeding relating to the dispute.

(c)   Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator. Each party shall treat information received from the other party pursuant to the mediation that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of such other party in accordance with Section 7.15.

(d)   If the parties have engaged in good faith participation in the mediation but have not resolved the dispute for any reason, either party or the mediator may terminate the mediation at any time and the dispute can then proceed to arbitration pursuant to Section 5.2 below. If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following the date of the notice delivered pursuant to Section 5.1(a), the mediation shall automatically terminate (unless extended by agreement of the parties) and the dispute can then proceed to arbitration pursuant to Section 5.2 below.

5.2   Arbitration. Disputes arising under or in connection with this Agreement that are not resolved pursuant to Section 5.1, including requests for specific performance, will be resolved through binding arbitration conducted pursuant to the rules of the International Court of Arbitration of the International Chamber of Commerce. The arbitration will be conducted in the English language and will occur in Los Angeles County, California. Any arbitration will be in front of a single arbitrator, unless (i) ICANN is seeking punitive or exemplary damages, or operational sanctions, (ii) the parties agree in writing to a greater number of arbitrators, or (iii) the dispute arises under Section 7.6 or 7.7. In the case of clauses (i), (ii) or (iii) in the preceding sentence, the arbitration will be in front of three arbitrators with each party selecting one arbitrator and the two selected arbitrators selecting the third arbitrator. In order to expedite the arbitration and limit its cost, the arbitrator(s) shall establish page limits for the parties' filings in conjunction with the arbitration, and should the arbitrator(s) determine that a hearing is necessary, the hearing shall be limited to one (1) calendar day, provided that in any arbitration in which ICANN is seeking punitive or exemplary damages, or operational sanctions, the hearing may be extended for one (1) additional calendar day if agreed upon by the parties or ordered by the arbitrator(s) based on the arbitrator(s) independent determination or the reasonable request of one of the parties thereto. The prevailing party in the arbitration will have the right to recover its costs and reasonable attorneys' fees, which the arbitrator(s) shall include in the awards. In the event the arbitrators determine that Registry Operator has been repeatedly and willfully in fundamental and material breach of its obligations set forth in Article 2, Article 6 or Section 5.4 of this Agreement, ICANN may request the arbitrators award punitive or exemplary damages, or operational sanctions (including without limitation an order temporarily restricting Registry Operator's right to sell new registrations). Each party shall treat information received from the other party pursuant to the arbitration that is appropriately marked as confidential (as required by Section 7.15) as Confidential Information of such other party in accordance with Section 7.15. In any

litigation involving ICANN concerning this Agreement, jurisdiction and exclusive venue for such litigation will be in a court located in Los Angeles County, California; however, the parties will also have the right to enforce a judgment of such a court in any court of competent jurisdiction.

5.3 **Limitation of Liability**. ICANN's aggregate monetary liability for violations of this Agreement will not exceed an amount equal to the Registry-Level Fees paid by Registry Operator to ICANN within the preceding twelve-month period pursuant to this Agreement (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any). Registry Operator's aggregate monetary liability to ICANN for breaches of this Agreement will be limited to an amount equal to the fees paid to ICANN during the preceding twelve-month period (excluding the Variable Registry-Level Fee set forth in Section 6.3, if any), and punitive and exemplary damages, if any, awarded in accordance with Section 5.2, except with respect to Registry Operator's indemnification obligations pursuant to Section 7.1 and Section 7.2. In no event shall either party be liable for special, punitive, exemplary or consequential damages arising out of or in connection with this Agreement or the performance or nonperformance of obligations undertaken in this Agreement, except as provided in Section 5.2. Except as otherwise provided in this Agreement, neither party makes any warranty, express or implied, with respect to the services rendered by itself, its servants or agents, or the results obtained from their work, including, without limitation, any implied warranty of merchantability, non-infringement or fitness for a particular purpose.

5.4 **Specific Performance**. Registry Operator and ICANN agree that irreparable damage could occur if any of the provisions of this Agreement was not performed in accordance with its specific terms. Accordingly, the parties agree that they each shall be entitled to seek from the arbitrator or court of competent jurisdiction specific performance of the terms of this Agreement (in addition to any other remedy to which each party is entitled).

ARTICLE 6.

FEES

6.1 **Registry-Level Fees.**

(a) Registry Operator shall pay ICANN a registry-level fee equal to (i) the registry fixed fee of US$6,250 per calendar quarter and (ii) the registry-level transaction fee (collectively, the "Registry-Level Fees"). The registry-level transaction fee will be equal to the number of annual increments of an initial or renewal domain name registration (at one or more levels, and including renewals associated with transfers from one ICANN-accredited registrar to another, each a "Transaction"), during the applicable calendar quarter multiplied by US$0.25; provided, however that the registry-level transaction fee shall not apply until and unless more than 50,000 Transactions have occurred in the TLD during any calendar quarter or any consecutive four calendar quarter period in the aggregate (the "Transaction Threshold") and shall apply to each Transaction that occurred

15

during each quarter in which the Transaction Threshold has been met, but shall not apply to each quarter in which the Transaction Threshold has not been met. Registry Operator's obligation to pay the quarterly registry-level fixed fee will begin on the date on which the TLD is delegated in the DNS to Registry Operator. The first quarterly payment of the registry-level fixed fee will be prorated based on the number of calendar days between the delegation date and the end of the calendar quarter in which the delegation date falls.

   (b) Subject to Section 6.1(a), Registry Operator shall pay the Registry-Level Fees on a quarterly basis to an account designated by ICANN within thirty (30) calendar days following the date of the invoice provided by ICANN.

   6.2 **Cost Recovery for RSTEP**. Requests by Registry Operator for the approval of Additional Services pursuant to Section 2.1 may be referred by ICANN to the Registry Services Technical Evaluation Panel ("RSTEP") pursuant to that process at http://www.icann.org/en/registries/rsep/. In the event that such requests are referred to RSTEP, Registry Operator shall remit to ICANN the invoiced cost of the RSTEP review within fourteen (14) calendar days of receipt of a copy of the RSTEP invoice from ICANN, unless ICANN determines, in its sole and absolute discretion, to pay all or any portion of the invoiced cost of such RSTEP review.

   6.3 **Variable Registry-Level Fee**.

   (a) If the ICANN accredited registrars (accounting, in the aggregate, for payment of two-thirds of all registrar-level fees (or such portion of ICANN accredited registrars necessary to approve variable accreditation fees under the then-current registrar accreditation agreement), do not approve, pursuant to the terms of their registrar accreditation agreements with ICANN, the variable accreditation fees established by the ICANN Board of Directors for any ICANN fiscal year, upon delivery of notice from ICANN, Registry Operator shall pay to ICANN a variable registry-level fee, which shall be paid on a fiscal quarter basis, and shall accrue as of the beginning of the first fiscal quarter of such ICANN fiscal year (the "Variable Registry-Level Fee"). The fee will be calculated and invoiced by ICANN on a quarterly basis, and shall be paid by Registry Operator within sixty (60) calendar days with respect to the first quarter of such ICANN fiscal year and within twenty (20) calendar days with respect to each remaining quarter of such ICANN fiscal year, of receipt of the invoiced amount by ICANN. The Registry Operator may invoice and collect the Variable Registry-Level Fees from the registrars that are party to a registry-registrar agreement with Registry Operator (which agreement may specifically provide for the reimbursement of Variable Registry-Level Fees paid by Registry Operator pursuant to this Section 6.3); provided, that the fees shall be invoiced to all ICANN accredited registrars if invoiced to any. The Variable Registry-Level Fee, if collectible by ICANN, shall be an obligation of Registry Operator and shall be due and payable as provided in this Section 6.3 irrespective of Registry Operator's ability to seek and obtain reimbursement of such fee from registrars. In the event ICANN later collects variable accreditation fees for which Registry Operator has paid ICANN a Variable Registry-Level Fee, ICANN shall reimburse the Registry Operator an appropriate amount of the Variable Registry-Level Fee, as reasonably determined by ICANN. If the ICANN accredited registrars (as a group) do approve,

pursuant to the terms of their registrar accreditation agreements with ICANN, the variable accreditation fees established by the ICANN Board of Directors for a fiscal year, ICANN shall not be entitled to a Variable-Level Fee hereunder for such fiscal year, irrespective of whether the ICANN accredited registrars comply with their payment obligations to ICANN during such fiscal year.

(b)   The amount of the Variable Registry-Level Fee will be specified for each registrar, and may include both a per-registrar component and a transactional component. The per-registrar component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year. The transactional component of the Variable Registry-Level Fee shall be specified by ICANN in accordance with the budget adopted by the ICANN Board of Directors for each ICANN fiscal year but shall not exceed US$0.25 per domain name registration (including renewals associated with transfers from one ICANN accredited registrar to another) per year.

6.4   Pass Through Fees. Registry Operator shall pay to ICANN (i) a one-time fee equal to US$5,000 for access to and use of the Trademark Clearinghouse as described in Specification 7 (the "RPM Access Fee") and (ii) an amount specified by ICANN not to exceed US$0.25 per Sunrise Registration and Claims Registration (as such terms are used in Trademark Clearinghouse RPMs incorporated herein pursuant to Specification 7) (the "RPM Registration Fee"). The RPM Access Fee will be invoiced as of the Effective Date of this Agreement, and Registry Operator shall pay such fee to an account specified by ICANN within thirty (30) calendar days following the date of the invoice. ICANN will invoice Registry Operator quarterly for the RPM Registration Fee, which shall be due in accordance with the invoicing and payment procedure specified in Section 6.1.

6.5   Adjustments to Fees. Notwithstanding any of the fee limitations set forth in this Article 6, commencing upon the expiration of the first year of this Agreement, and upon the expiration of each year thereafter during the Term, the then-current fees set forth in Section 6.1 and Section 6.3 may be adjusted, at ICANN's discretion, by a percentage equal to the percentage change, if any, in (i) the Consumer Price Index for All Urban Consumers, U.S. City Average (1982-1984 = 100) published by the United States Department of Labor, Bureau of Labor Statistics, or any successor index (the "CPI") for the month which is one (1) month prior to the commencement of the applicable year, over (ii) the CPI published for the month which is one (1) month prior to the commencement of the immediately prior year. In the event of any such increase, ICANN shall provide notice to Registry Operator specifying the amount of such adjustment. Any fee adjustment under this Section 6.5 shall be effective as of the first day of the first calendar quarter following at least thirty (30) days after ICANN's delivery to Registry Operator of such fee adjustment notice.

6.6   Additional Fee on Late Payments. For any payments thirty (30) calendar days or more overdue under this Agreement, Registry Operator shall pay an additional fee on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law.

ARTICLE 7.

MISCELLANEOUS

7.1 Indemnification of ICANN.

(a)   Registry Operator shall indemnify and defend ICANN and its directors, officers, employees, and agents (collectively, "Indemnitees") from and against any and all third-party claims, damages, liabilities, costs, and expenses, including reasonable legal fees and expenses, arising out of or relating to intellectual property ownership rights with respect to the TLD, the delegation of the TLD to Registry Operator, Registry Operator's operation of the registry for the TLD or Registry Operator's provision of Registry Services, provided that Registry Operator shall not be obligated to indemnify or defend any Indemnitee to the extent the claim, damage, liability, cost or expense arose: (i) due to the actions or omissions of ICANN, its subcontractors, panelists or evaluators specifically related to and occurring during the registry TLD application process (other than actions or omissions requested by or for the benefit of Registry Operator), or (ii) due to a breach by ICANN of any obligation contained in this Agreement or any willful misconduct by ICANN. This Section shall not be deemed to require Registry Operator to reimburse or otherwise indemnify ICANN for costs associated with the negotiation or execution of this Agreement, or with monitoring or management of the parties' respective obligations hereunder. Further, this Section shall not apply to any request for attorney's fees in connection with any litigation or arbitration between or among the parties, which shall be governed by Article 5 or otherwise awarded by a court of competent jurisdiction or arbitrator.

(b)   For any claims by ICANN for indemnification whereby multiple registry operators (including Registry Operator) have engaged in the same actions or omissions that gave rise to the claim, Registry Operator's aggregate liability to indemnify ICANN with respect to such claim shall be limited to a percentage of ICANN's total claim, calculated by dividing the number of total domain names under registration with Registry Operator within the TLD (which names under registration shall be calculated consistently with Article 6 hereof for any applicable quarter) by the total number of domain names under registration within all top level domains for which the registry operators thereof are engaging in the same acts or omissions giving rise to such claim. For the purposes of reducing Registry Operator's liability under Section 7.1(a) pursuant to this Section 7.1(b), Registry Operator shall have the burden of identifying the other registry operators that are engaged in the same actions or omissions that gave rise to the claim, and demonstrating, to ICANN's reasonable satisfaction, such other registry operators' culpability for such actions or omissions. For the avoidance of doubt, in the event that a registry operator is engaged in the same acts or omissions giving rise to the claims, but such registry operator(s) do not have the same or similar indemnification obligations to ICANN as set forth in Section 7.1(a) above, the number of domains under management by such registry operator(s) shall nonetheless be included in the calculation in the preceding sentence.

7.2 Indemnification Procedures. If any third-party claim is commenced that is indemnified under Section 7.1 above, ICANN shall provide notice thereof to Registry

Operator as promptly as practicable. Registry Operator shall be entitled, if it so elects, in a notice promptly delivered to ICANN, to immediately take control of the defense and investigation of such claim and to employ and engage attorneys reasonably acceptable to ICANN to handle and defend the same, at Registry Operator's sole cost and expense, provided that in all events ICANN will be entitled to control at its sole cost and expense the litigation of issues concerning the validity or interpretation of ICANN's policies, Bylaws or conduct. ICANN shall cooperate, at Registry Operator's cost and expense, in all reasonable respects with Registry Operator and its attorneys in the investigation, trial, and defense of such claim and any appeal arising therefrom, and may, at its own cost and expense, participate, through its attorneys or otherwise, in such investigation, trial and defense of such claim and any appeal arising therefrom. No settlement of a claim that involves a remedy affecting ICANN other than the payment of money in an amount that is fully indemnified by Registry Operator will be entered into without the consent of ICANN. If Registry Operator does not assume full control over the defense of a claim subject to such defense in accordance with this Section 7.2, ICANN will have the right to defend the claim in such manner as it may deem appropriate, at the cost and expense of Registry Operator and Registry Operator shall cooperate in such defense.

7.3   **Defined Terms**. For purposes of this Agreement, unless such definitions are amended pursuant to a Consensus Policy at a future date, in which case the following definitions shall be deemed amended and restated in their entirety as set forth in such Consensus Policy, Security and Stability shall be defined as follows:

(a)   For the purposes of this Agreement, an effect on "Security" shall mean (1) the unauthorized disclosure, alteration, insertion or destruction of registry data, or (2) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.

(b)   For purposes of this Agreement, an effect on "Stability" shall refer to (1) lack of compliance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice Requests for Comments ("RFCs") sponsored by the Internet Engineering Task Force; or (2) the creation of a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established and recognized Internet standards body, such as the relevant Standards-Track or Best Current Practice RFCs, and relying on Registry Operator's delegated information or provisioning of services.

7.4   **No Offset**. All payments due under this Agreement will be made in a timely manner throughout the Term and notwithstanding the pendency of any dispute (monetary or otherwise) between Registry Operator and ICANN.

7.5   **Change of Control; Assignment and Subcontracting**. Except as set forth in this Section 7.5, neither party may assign any of its rights and obligations under this Agreement without the prior written approval of the other party, which approval will not

be unreasonably withheld. For purposes of this Section 7.5, a direct or indirect change of control of Registry Operator or any subcontracting arrangement that relates to any Critical Function (as identified in Section 6 of Specification 10) for the TLD (a "Material Subcontracting Arrangement") shall be deemed an assignment.

       (a)   Registry Operator must provide no less than thirty (30) calendar days advance notice to ICANN of any assignment or Material Subcontracting Arrangement, and any agreement to assign or subcontract any portion of the operations of the TLD (whether or not a Material Subcontracting Arrangement) must mandate compliance with all covenants, obligations and agreements by Registry Operator hereunder, and Registry Operator shall continue to be bound by such covenants, obligations and agreements. Registry Operator must also provide no less than thirty (30) calendar days advance notice to ICANN prior to the consummation of any transaction anticipated to result in a direct or indirect change of control of Registry Operator.

       (b)   Within thirty (30) calendar days of either such notification pursuant to Section 7.5(a), ICANN may request additional information from Registry Operator establishing (i) compliance with this Agreement and (ii) that the party acquiring such control or entering into such assignment or Material Subcontracting Arrangement (in any case, the "Contracting Party") and the ultimate parent entity of the Contracting Party meets the ICANN-adopted specification or policy on registry operator criteria then in effect (including with respect to financial resources and operational and technical capabilities), in which case Registry Operator must supply the requested information within fifteen (15) calendar days.

       (c)   Registry Operator agrees that ICANN's consent to any assignment, change of control or Material Subcontracting Arrangement will also be subject to background checks on any proposed Contracting Party (and such Contracting Party's Affiliates).

       (d)   If ICANN fails to expressly provide or withhold its consent to any assignment, direct or indirect change of control of Registry Operator or any Material Subcontracting Arrangement within thirty (30) calendar days of ICANN's receipt of notice of such transaction (or, if ICANN has requested additional information from Registry Operator as set forth above, thirty (30) calendar days of the receipt of all requested written information regarding such transaction) from Registry Operator, ICANN shall be deemed to have consented to such transaction.

       (e)   In connection with any such assignment, change of control or Material Subcontracting Arrangement, Registry Operator shall comply with the Registry Transition Process.

       (f)   Notwithstanding the foregoing, (i) any consummated change of control shall not be voidable by ICANN; provided, however, that, if ICANN reasonably determines to withhold its consent to such transaction, ICANN may terminate this Agreement pursuant to Section 4.3(g), (ii) ICANN may assign this Agreement without the

consent of Registry Operator upon approval of the ICANN Board of Directors in conjunction with a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (iii) Registry Operator may assign this Agreement without the consent of ICANN directly to a wholly-owned subsidiary of Registry Operator, or, if Registry Operator is a wholly-owned subsidiary, to its direct parent or to another wholly-owned subsidiary of its direct parent, upon such subsidiary's or parent's, as applicable, express assumption of the terms and conditions of this Agreement, and (iv) ICANN shall be deemed to have consented to any assignment, Material Subcontracting Arrangement or change of control transaction in which the Contracting Party is an existing operator of a generic top-level domain pursuant to a registry agreement between such Contracting Party and ICANN (provided that such Contracting Party is then in compliance with the terms and conditions of such registry agreement in all material respects), unless ICANN provides to Registry Operator a written objection to such transaction within ten (10) calendar days of ICANN's receipt of notice of such transaction pursuant to this Section 7.5. Notwithstanding Section 7.5(a), in the event an assignment is made pursuant to clauses (ii) or (iii) of this Section 7.5(f), the assigning party will provide the other party with prompt notice following any such assignment.

7.6   **Amendments and Waivers**.

(a)   If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein) and all other registry agreements between ICANN and the Applicable Registry Operators (the "Applicable Registry Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 7.6; provided that a Special Amendment may not be a Restricted Amendment.

(b)   Prior to submitting a Special Amendment for Registry Operator Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registry Operators in accordance with Section 7.9. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registry Operators).

(c)   If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registry Operators. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable

Registry Operators, such Special Amendment receives Registry Operator Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registry Operators, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registry Operator (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registry Operator Approval, the Special Amendment shall be deemed not approved by the Applicable Registry Operators (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

(d)   If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of Specification 1, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registry Operator shall comply with its obligations pursuant to Section 2.2 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 7.6(d), the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject matter of such Rejected Amendment was the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

(e)   If (a) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of Specification 1, (b) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registry Operator Approval pursuant to Section 7.6(c), the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (c) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (A) recommends adoption of the Rejected Amendment as Consensus Policy or (B) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

(i)   the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

(ii)   the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

(iii)   to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registry Operators, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

(iv)   the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

(v)   following such public comment period, the ICANN Board of Directors must (a) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty (60) calendar days; and (b) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registry Operator Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 7.6(f), be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registry Operator (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registry fees charged by ICANN hereunder, or amend this Section 7.6.

(f)   Notwithstanding the provisions of Section 7.6(e), a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registry Operators, submits to the ICANN Board of Directors an alternative to the Board Amendment (an "Alternative Amendment") that meets the following requirements:

(i)   sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

(ii)   addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

(iii)   compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registry Operators, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses (i) through (iii) in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registry Operator Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registry Operator, which effective date shall deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registry Operator Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registry Operator Approval within thirty (30) calendar days of submission of such Alternative Amendment to the Applicable Registry Operators (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registry Operator (which

effective date shall deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 7.6(f)(i) through 7.6(f)(iii). The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 7.6(e)(i) through 7.6(e)(v).

(g)   In the event that Registry Operator believes an Approved Amendment does not meet the substantive requirements set out in this Section 7.6 or has been adopted in contravention of any of the procedural provisions of this Section 7.6, Registry Operator may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Article 5, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registry Operator of the Approved Amendment, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

(h)   Registry Operator may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registry Operator hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registry Operator of such Approved Amendment. Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registry Operator. An Exemption Request may only be granted upon a clear and convincing showing by Registry Operator that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registry Operator. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants. Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement. If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registry Operator may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Article 5. The Approved Amendment will be

deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registry Operator that are approved by ICANN pursuant to this Section 7.6(j), agreed to by ICANN following mediation pursuant to Section 5.1 or through an arbitration decision pursuant to Section 5.2 shall exempt Registry Operator from any Approved Amendment, and no Exemption Request granted to any other Applicable Registry Operator (whether by ICANN or through arbitration) shall have any effect under this Agreement or exempt Registry Operator from any Approved Amendment.

(i)   Except as set forth in this Section 7.6, Section 7.7 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 7.6 or Section 7.7 shall restrict ICANN and Registry Operator from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to enforce any of the provisions hereof shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Sections 7.6 or 7.7 shall be deemed to limit Registry Operator's obligation to comply with Section 2.2.

(j)   For purposes of this Section 7.6, the following terms shall have the following meanings:

(i)   "Applicable Registry Operators" means, collectively, the registry operators of top-level domains party to a registry agreement that contains a provision similar to this Section 7.6, including Registry Operator.

(ii)   "Registry Operator Approval" means the receipt of each of the following: (A) the affirmative approval of the Applicable Registry Operators whose payments to ICANN accounted for two-thirds of the total amount of fees (converted to U.S. dollars, if applicable, at the prevailing exchange rate published the prior day in the U.S. Edition of the Wall Street Journal for the date such calculation is made by ICANN) paid to ICANN by all the Applicable Registry Operators during the immediately previous calendar year pursuant to the Applicable Registry Agreements, and (B) the affirmative approval of a majority of the Applicable Registry Operators at the time such approval is obtained. For the avoidance of doubt, with respect to clause (B), each Applicable Registry Operator shall have one vote for each top-level domain operated by such Registry Operator pursuant to an Applicable Registry Agreement.

(iii)   "Restricted Amendment" means the following: (A) an amendment of Specification 1, (B) except to the extent addressed in Section

2.10 hereof, an amendment that specifies the price charged by Registry Operator to registrars for domain name registrations, (C) an amendment to the definition of Registry Services as set forth in the first paragraph of Section 2.1 of Specification 6, or (D) an amendment to the length of the Term.

(iv) "Substantial and Compelling Reason in the Public Interest" means a reason that is justified by an important, specific, and articulated public interest goal that is within ICANN's mission and consistent with a balanced application of ICANN's core values as defined in ICANN's Bylaws.

(v) "Working Group" means representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements (excluding bilateral amendments pursuant to Section 7.6(i)).

(k) Notwithstanding anything in this Section 7.6 to the contrary, (i) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for Approved Amendment to become effective with respect to Registry Operator, and (ii) no Approved Amendment adopted pursuant to Section 7.6 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.7 **Negotiation Process**.

(a) If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registry Stakeholder Group ("Chair") desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a "Negotiation Notice"). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.7 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve (12) month period beginning on July 1, 2014.

(b) Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group (as defined in Section 7.6) shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the "Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the "Discussion Period").

(c) If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed

Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval (as defined in Section 7.6) and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(d)   If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

(i)   The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law, who has no ongoing business relationship with either party and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registry Operator. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.7(d)(i).

(ii)   The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

(iii)   Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

(iv)   If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registry Operators in accordance with Section 7.9. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registry Operator Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment (as defined in Section 7.6) by the Applicable Registry Operators and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator.

(v)   If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.7(e)(ii) below.

(e)   If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.2, subject to the requirements and limitations of this Section 7.7(e).

(i)   If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, the Working Group or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registry Operators), and information regarding such comments and consideration shall be provided to a three (3) person arbitrator panel. Each party may modify its Proposed Revisions before and after the Posting Period. The arbitration proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registry operators (including Registry Operator) into a single proceeding. Except as set forth in this Section 7.7, the arbitration shall be conducted pursuant to Section 5.2.

(ii)   No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed

Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of Specification 1, or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Articles 1, 3 and 6; Sections 2.1, 2.2, 2.5, 2.7, 2.9, 2.10, 2.16, 2.17, 2.19, 4.1, 4.2, 7.3, 7.6, 7.7, 7.8, 7.10, 7.11, 7.12, 7.13, 7.14, 7.16; Section 2.8 and Specification 7 (but only to the extent such Proposed Revisions seek to implement an RPM not contemplated by Sections 2.8 and Specification 7); Exhibit A; and Specifications 1, 4, 6, 10 and 11.

(iii)   The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

(iv)   No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registry Operator Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

(v)   In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registry Operators and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registry Operator and deemed an Approved Amendment hereunder.

(f)   With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registry may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 7.6.

(g)   Notwithstanding anything in this Section 7.7 to the contrary, (a) if Registry Operator provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registry Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registry Operator, and (b) no Approved Amendment adopted pursuant to Section 7.7 shall become effective with respect to Registry Operator if Registry Operator provides ICANN with an irrevocable notice of termination pursuant to Section 4.4(b).

7.8 **No Third-Party Beneficiaries**. This Agreement will not be construed to create any obligation by either ICANN or Registry Operator to any non-party to this Agreement, including any registrar or registered name holder.

7.9 **General Notices**. Except for notices pursuant to Sections 7.6 and 7.7, all notices to be given under or in relation to this Agreement will be given either (i) in writing at the address of the appropriate party as set forth below or (ii) via facsimile or electronic mail as provided below, unless that party has given a notice of change of postal or email address, or facsimile number, as provided in this Agreement. All notices under Sections 7.6 and 7.7 shall be given by both posting of the applicable information on ICANN's web site and transmission of such information to Registry Operator by electronic mail. Any change in the contact information for notice below will be given by the party within thirty (30) calendar days of such change. Other than notices under Sections 7.6 or 7.7, any notice required by this Agreement will be deemed to have been properly given (i) if in paper form, when delivered in person or via courier service with confirmation of receipt or (ii) if via facsimile or by electronic mail, upon confirmation of receipt by the recipient's facsimile machine or email server, provided that such notice via facsimile or electronic mail shall be followed by a copy sent by regular postal mail service within three (3) calendar days. Any notice required by Sections 7.6 or 7.7 will be deemed to have been given when electronically posted on ICANN's website and upon confirmation of receipt by the email server. In the event other means of notice become practically achievable, such as notice via a secure website, the parties will work together to implement such notice means under this Agreement.

> If to ICANN, addressed to:
> Internet Corporation for Assigned Names and Numbers
> 12025 Waterfront Drive, Suite 300
> Los Angeles, CA 90094-2536
> USA
> Telephone: +1-310-301-5800
> Facsimile: +1-310-823-8649
> Attention: President and CEO
>
> With a Required Copy to: General Counsel
> Email: (As specified from time to time.)
>
> If to Registry Operator, addressed to:
> Spring Fields, LLC
> c/o Donuts Inc.
> 10500 NE 8th Street, Suite 350
> Bellevue, Washington 98004
> USA
> Telephone: Contact nformation Redacted
> Facsimile: Contact nformation Redacted
> Attention: Jonathon Nevett, Executive Vice President
> Email: Contact Information Redacted

7.10   Entire Agreement. This Agreement (including those specifications and documents incorporated by reference to URL locations which form a part of it) constitutes the entire agreement of the parties hereto pertaining to the operation of the TLD and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

7.11   English Language Controls. Notwithstanding any translated version of this Agreement and/or specifications that may be provided to Registry Operator, the English language version of this Agreement and all referenced specifications are the official versions that bind the parties hereto. In the event of any conflict or discrepancy between any translated version of this Agreement and the English language version, the English language version controls. Notices, designations, determinations, and specifications made under this Agreement shall be in the English language.

7.12   Ownership Rights. Nothing contained in this Agreement shall be construed as (a) establishing or granting to Registry Operator any property ownership rights or interests of Registry Operator in the TLD or the letters, words, symbols or other characters making up the TLD string, or (b) affecting any existing intellectual property or ownership rights of Registry Operator.

7.13   Severability; Conflicts with Laws. This Agreement shall be deemed severable; the invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of the balance of this Agreement or of any other term hereof, which shall remain in full force and effect. If any of the provisions hereof are determined to be invalid or unenforceable, the parties shall negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible. ICANN and the Working Group will mutually cooperate to develop an ICANN procedure for ICANN's review and consideration of alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement. Until such procedure is developed and implemented by ICANN, ICANN will review and consider alleged conflicts between applicable laws and non-WHOIS related provisions of this Agreement in a manner similar to ICANN's Procedure For Handling WHOIS Conflicts with Privacy Law.

7.14   Court Orders. ICANN will respect any order from a court of competent jurisdiction, including any orders from any jurisdiction where the consent or non-objection of the government was a requirement for the delegation of the TLD. Notwithstanding any other provision of this Agreement, ICANN's implementation of any such order will not be a breach of this Agreement

7.15   Confidentiality

(a)   Subject to Section 7.15(c), during the Term and for a period of three (3) years thereafter, each party shall, and shall cause its and its Affiliates' officers, directors, employees and agents to, keep confidential and not publish or otherwise disclose to any third party, directly or indirectly, any information that is, and the disclosing party has marked as, or has otherwise designated in writing to the receiving party as, "confidential

trade secret," "confidential commercial information" or "confidential financial information" (collectively, "Confidential Information"), except to the extent such disclosure is permitted by the terms of this Agreement.

(b)   The confidentiality obligations under Section 7.15(a) shall not apply to any Confidential Information that (i) is or hereafter becomes part of the public domain by public use, publication, general knowledge or the like through no fault of the receiving party in breach of this Agreement, (ii) can be demonstrated by documentation or other competent proof to have been in the receiving party's possession prior to disclosure by the disclosing party without any obligation of confidentiality with respect to such information, (iii) is subsequently received by the receiving party from a third party who is not bound by any obligation of confidentiality with respect to such information, (iv) has been published by a third party or otherwise enters the public domain through no fault of the receiving party, or (v) can be demonstrated by documentation or other competent evidence to have been independently developed by or for the receiving party without reference to the disclosing party's Confidential Information.

(c)   Each party shall have the right to disclose Confidential Information to the extent that such disclosure is (i) made in response to a valid order of a court of competent jurisdiction or, if in the reasonable opinion of the receiving party's legal counsel, such disclosure is otherwise required by applicable law; provided, however, that the receiving party shall first have given notice to the disclosing party and given the disclosing party a reasonable opportunity to quash such order or to obtain a protective order or confidential treatment order requiring that the Confidential Information that is the subject of such order or other applicable law be held in confidence by such court or other third party recipient, unless the receiving party is not permitted to provide such notice under such order or applicable law, or (ii) made by the receiving party or any of its Affiliates to its or their attorneys, auditors, advisors, consultants, contractors or other third parties for use by such person or entity as may be necessary or useful in connection with the performance of the activities under this Agreement, provided that such third party is bound by confidentiality obligations at least as stringent as those set forth herein, either by written agreement or through professional responsibility standards.

* * * * *

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By: _____

Akram Atallah
President and CEO

Spring Fields, LLC

By: _____

Paul Stahura
President and CEO

EXHIBIT A

Approved Services

The ICANN gTLD Applicant Guidebook (located at http://newgtlds.icann.org/en/applicants/agb) and the RSEP specify processes for consideration of proposed registry services. Registry Operator may provide any service that is required by the terms of this Agreement. In addition, the following services (if any) are specifically identified as having been approved by ICANN prior to the effective date of the Agreement, and Registry Operator may provide such services:

1. **DNS Service – TLD Zone Contents**

   Notwithstanding anything else in this Agreement, as indicated in section 2.2.3.3 of the gTLD Applicant Guidebook, permissible contents for the TLD's zone are:

   1.1. Apex SOA record

   1.2. Apex NS records and in-bailiwick glue for the TLD's DNS servers

   1.3. NS records and in-bailiwick glue for DNS servers of registered names in the TLD

   1.4. DS records for registered names in the TLD

   1.5. Records associated with signing the TLD zone (i.e., RRSIG, DNSKEY, NSEC, and NSEC3)

   (Note: The above language effectively does not allow, among other things, the inclusion of DNS resource records that would enable a dotless domain name (e.g., apex A, AAAA, MX records) in the TLD zone.)

   If Registry Operator wishes to place any DNS resource record type into its TLD DNS zone (other than those listed in Sections 1.1 through 1.5 above), it must describe in detail its proposal and submit a Registry Services Evaluation Process (RSEP) request. This will be evaluated per RSEP to determine whether the service would create a risk of a meaningful adverse impact on security or stability of the DNS. Registry Operator recognizes and acknowledges that a service based on the use of less-common DNS resource records in the TLD zone, even if approved, might not work as intended for all users due to lack of software support.

2. **Internationalized Domain Names (IDNs)**

   Registry Operator may offer registration of IDNs at the second and lower levels provided that Registry Operator complies with the following requirements:

   2.1. Registry Operator must offer Registrars support for handling IDN registrations in EPP.

2.2. Registry Operator must handle variant IDNs as follows:

2.2.1. Variant IDNs (as defined in the Registry Operator's IDN tables and IDN Registration Rules) will be blocked from registration.

2.3. Registry Operator may offer registration of IDNs in the following languages/scripts (IDN Tables and IDN Registration Rules will be published by the Registry Operator as specified in the ICANN IDN Implementation Guidelines):

2.3.1. Chinese Language

3. Searchable Whois

Notwithstanding anything else in this Agreement, Registry Operator must offer a searchable Whois service compliant with the requirements described in Section 1.10 of Specification 4 of this Agreement. Registry Operator must make available the services only to authenticated users after they logged in by supplying proper credentials (i.e., user name and password). Registry Operator must issue such credentials exclusively to eligible users and institutions that supply sufficient proof of their legitimate interest in this feature (e.g., law enforcement agencies).

SPECIFICATION 1

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. **Consensus Policies**.

    1.1.   "***Consensus Policies***" are those policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this Specification. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with the process set forth therein.

    1.2.   Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including the operators of gTLDs. Consensus Policies shall relate to one or more of the following:

    1.2.1   issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or Domain Name System ("DNS");

    1.2.2   functional and performance specifications for the provision of Registry Services;

    1.2.3   Security and Stability of the registry database for the TLD;

    1.2.4   registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars;

    1.2.5   resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or

    1.2.6   restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated.

    1.3.   Such categories of issues referred to in Section 1.2 of this Specification shall include, without limitation:

    1.3.1   principles for allocation of registered names in the TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);

    1.3.2   prohibitions on warehousing of or speculation in domain names by registries or registrars;

1.3.3 reservation of registered names in the TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration); and

1.3.4 maintenance of and access to accurate and up-to-date information concerning domain name registrations; and procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility for serving registered domain names in a TLD affected by such a suspension or termination.

1.4. In addition to the other limitations on Consensus Policies, they shall not:

1.4.1 prescribe or limit the price of Registry Services;

1.4.2 modify the terms or conditions for the renewal or termination of the Registry Agreement;

1.4.3 modify the limitations on Temporary Policies (defined below) or Consensus Policies;

1.4.4 modify the provisions in the registry agreement regarding fees paid by Registry Operator to ICANN; or

1.4.5 modify ICANN's obligations to ensure equitable treatment of registry operators and act in an open and transparent manner.

2. **Temporary Policies**. Registry Operator shall comply with and implement all specifications or policies established by the Board on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registry Services or the DNS ("***Temporary Policies***").

2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.

2.1.1 ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why

the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.

2.1.2   If the period of time for which the Temporary Policy is adopted exceeds ninety (90) calendar days, the Board shall reaffirm its temporary adoption every ninety (90) calendar days for a total period not to exceed one (1) year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one (1) year period expires or, if during such one (1) year period, the Temporary Policy does not become a Consensus Policy and is not reaffirmed by the Board, Registry Operator shall no longer be required to comply with or implement such Temporary Policy.

3.   **Notice and Conflicts**. Registry Operator shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between Registry Services and Consensus Policies or any Temporary Policy, the Consensus Polices or Temporary Policy shall control, but only with respect to subject matter in conflict.

SPECIFICATION 2

DATA ESCROW REQUIREMENTS

Registry Operator will engage an independent entity to act as data escrow agent ("***Escrow Agent***") for the provision of data escrow services related to the Registry Agreement. The following Technical Specifications set forth in Part A, and Legal Requirements set forth in Part B, will be included in any data escrow agreement between Registry Operator and the Escrow Agent, under which ICANN must be named a third-party beneficiary. In addition to the following requirements, the data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms provided below.

PART A – TECHNICAL SPECIFICATIONS

1. **Deposits**. There will be two types of Deposits: Full and Differential. For both types, the universe of Registry objects to be considered for data escrow are those objects necessary in order to offer all of the approved Registry Services.

    1.1. "**Full Deposit**" will consist of data that reflects the state of the registry as of 00:00:00 UTC (Coordinated Universal Time) on the day that such Full Deposit is submitted to Escrow Agent.

    1.2. "**Differential Deposit**" means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database transactions since the previous Deposit was completed as of 00:00:00 UTC of each day, but Sunday. Differential Deposits must include complete Escrow Records as specified below that were not included or changed since the most recent full or Differential Deposit (i.e., newly added or modified domain names).

2. **Schedule for Deposits**. Registry Operator will submit a set of escrow files on a daily basis as follows:

    2.1. Each Sunday, a Full Deposit must be submitted to the Escrow Agent by 23:59 UTC.

    2.2. The other six (6) days of the week, a Full Deposit or the corresponding Differential Deposit must be submitted to Escrow Agent by 23:59 UTC.

3. **Escrow Format Specification**.

    3.1. **Deposit's Format**. Registry objects, such as domains, contacts, name servers, registrars, etc. will be compiled into a file constructed as described in draft-arias-noguchi-registry-data-escrow, see Part A, Section 9, reference 1 of this Specification and draft-arias-noguchi-dnrd-objects-mapping, see Part A, Section 9, reference 2 of this Specification (collectively, the "DNDE Specification"). The DNDE Specification describes some elements as

optional; Registry Operator will include those elements in the Deposits if they are available. If not already an RFC, Registry Operator will use the most recent draft version of the DNDE Specification available at the Effective Date. Registry Operator may at its election use newer versions of the DNDE Specification after the Effective Date. Once the DNDE Specification is published as an RFC, Registry Operator will implement that version of the DNDE Specification, no later than one hundred eighty (180) calendar days after. UTF-8 character encoding will be used.

3.2.   **Extensions**. If a Registry Operator offers additional Registry Services that require submission of additional data, not included above, additional "extension schemas" shall be defined in a case by case basis to represent that data. These "extension schemas" will be specified as described in Part A, Section 9, reference 2 of this Specification. Data related to the "extensions schemas" will be included in the deposit file described in Part A, Section 3.1 of this Specification. ICANN and the respective Registry Operator shall work together to agree on such new objects' data escrow specifications.

4.   **Processing of Deposit files**. The use of compression is recommended in order to reduce electronic data transfer times, and storage capacity requirements. Data encryption will be used to ensure the privacy of registry escrow data. Files processed for compression and encryption will be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see Part A, Section 9, reference 3 of this Specification. Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC 4880, not marked as deprecated in OpenPGP IANA Registry, see Part A, Section 9, reference 4 of this Specification, that are also royalty-free. The process to follow for the data file in original text format is:

(1)   The XML file of the deposit as described in Part A, Section 9, reference 1 of this Specification must be named as the containing file as specified in Section 5 but with the extension xml.

(2)   The data file(s) are aggregated in a tarball file named the same as (1) but with extension tar.

(3)   A compressed and encrypted OpenPGP Message is created using the tarball file as sole input. The suggested algorithm for compression is ZIP as per RFC 4880. The compressed data will be encrypted using the escrow agent's public key. The suggested algorithms for Public-key encryption are Elgamal and RSA as per RFC 4880. The suggested algorithms for Symmetric-key encryption are TripleDES, AES128 and CAST5 as per RFC 4880.

(4)   The file may be split as necessary if, once compressed and encrypted, it is larger than the file size limit agreed with the escrow agent. Every part of a

split file, or the whole file if not split, will be called a processed file in this section.

(5)   A digital signature file will be generated for every processed file using the Registry Operator's private key. The digital signature file will be in binary OpenPGP format as per RFC 4880 Section 9, reference 3, and will not be compressed or encrypted. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.

(6)   The processed files and digital signature files will then be transferred to the Escrow Agent through secure electronic mechanisms, such as, SFTP, SCP, HTTPS file upload, etc. as agreed between the Escrow Agent and the Registry Operator. Non-electronic delivery through a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices may be used if authorized by ICANN.

(7)   The Escrow Agent will then validate every (processed) transferred data file using the procedure described in Part A, Section 8 of this Specification.

5.   **File Naming Conventions**. Files will be named according to the following convention: {gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext} where:

5.1.   {gTLD} is replaced with the gTLD name; in case of an IDN-TLD, the ASCII-compatible form (A-Label) must be used;

5.2.   {YYYY-MM-DD} is replaced by the date corresponding to the time used as a timeline watermark for the transactions; i.e. for the Full Deposit corresponding to 2009-08-02T00:00Z, the string to be used would be "2009-08-02";

5.3.   {type} is replaced by:

(1)   "full", if the data represents a Full Deposit;

(2)   "diff", if the data represents a Differential Deposit;

(3)   "thin", if the data represents a Bulk Registration Data Access file, as specified in Section 3 of Specification 4;

5.4.   {#} is replaced by the position of the file in a series of files, beginning with "1"; in case of a lone file, this must be replaced by "1".

5.5.   {rev} is replaced by the number of revision (or resend) of the file beginning with "0":

5.6.   {ext} is replaced by "sig" if it is a digital signature file of the quasi-homonymous file. Otherwise it is replaced by "ryde".

6.   **Distribution of Public Keys**. Each of Registry Operator and Escrow Agent will distribute its public key to the other party (Registry Operator or Escrow Agent, as the case may be) via email to an email address to be specified. Each party will confirm receipt of the other party's public key with a reply email, and the distributing party will subsequently reconfirm the authenticity of the key transmitted via offline methods, like in person meeting, telephone, etc. In this way, public key transmission is authenticated to a user able to send and receive mail via a mail server operated by the distributing party. Escrow Agent, Registry Operator and ICANN will exchange public keys by the same procedure.

7.   **Notification of Deposits**. Along with the delivery of each Deposit, Registry Operator will deliver to Escrow Agent and to ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification (the "Interface Specification")) a written statement (which may be by authenticated e-mail) that includes a copy of the report generated upon creation of the Deposit and states that the Deposit has been inspected by Registry Operator and is complete and accurate. Registry Operator will include the Deposit's "id" and "resend" attributes in its statement. The attributes are explained in Part A, Section 9, reference 1 of this Specification.

If not already an RFC, Registry Operator will use the most recent draft version of the Interface Specification at the Effective Date. Registry Operator may at its election use newer versions of the Interface Specification after the Effective Date. Once the Interface Specification is published as an RFC, Registry Operator will implement that version of the Interface Specification, no later than one hundred eighty (180) calendar days after such publishing.

8.   **Verification Procedure**.

(1)   The signature file of each processed file is validated.

(2)   If processed files are pieces of a bigger file, the latter is put together.

(3)   Each file obtained in the previous step is then decrypted and uncompressed.

(4)   Each data file contained in the previous step is then validated against the format defined in Part A, Section 9, reference 1 of this Specification.

(5)   If Part A, Section 9, reference 1 of this Specification includes a verification process, that will be applied at this step.

If any discrepancy is found in any of the steps, the Deposit will be considered incomplete.

9. **References**.

(1) Domain Name Data Escrow Specification (work in progress),
http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow

(2) Domain Name Registration Data (DNRD) Objects Mapping,
http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping

(3) OpenPGP Message Format, http://www.rfc-editor.org/rfc/rfc4880.txt

(4) OpenPGP parameters,
http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml

(5) ICANN interfaces for registries and data escrow agents,
http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces

PART B – LEGAL REQUIREMENTS

1. **Escrow Agent**. Prior to entering into an escrow agreement, the Registry Operator must provide notice to ICANN as to the identity of the Escrow Agent, and provide ICANN with contact information and a copy of the relevant escrow agreement, and all amendments thereto. In addition, prior to entering into an escrow agreement, Registry Operator must obtain the consent of ICANN to (a) use the specified Escrow Agent, and (b) enter into the form of escrow agreement provided. ICANN must be expressly designated as a third-party beneficiary of the escrow agreement. ICANN reserves the right to withhold its consent to any Escrow Agent, escrow agreement, or any amendment thereto, all in its sole discretion.

2. **Fees**. Registry Operator must pay, or have paid on its behalf, fees to the Escrow Agent directly. If Registry Operator fails to pay any fee by the due date(s), the Escrow Agent will give ICANN written notice of such non-payment and ICANN may pay the past-due fee(s) within fifteen (15) calendar days after receipt of the written notice from Escrow Agent. Upon payment of the past-due fees by ICANN, ICANN shall have a claim for such amount against Registry Operator, which Registry Operator shall be required to submit to ICANN together with the next fee payment due under the Registry Agreement.

3. **Ownership**. Ownership of the Deposits during the effective term of the Registry Agreement shall remain with Registry Operator at all times. Thereafter, Registry Operator shall assign any such ownership rights (including intellectual property rights, as the case may be) in such Deposits to ICANN. In the event that during the term of the Registry Agreement any Deposit is released from escrow to ICANN, any intellectual property rights held by Registry Operator in the Deposits will automatically be licensed to ICANN or to a party designated in writing by ICANN on a non-exclusive, perpetual, irrevocable, royalty-free, paid-up basis, for any use related to the operation, maintenance or transition of the TLD.

4. **Integrity and Confidentiality**. Escrow Agent will be required to (i) hold and maintain the Deposits in a secure, locked, and environmentally safe facility, which is accessible only to authorized representatives of Escrow Agent, (ii) protect the integrity and confidentiality of the Deposits using commercially reasonable measures and (iii) keep and safeguard each Deposit for one (1) year. ICANN and Registry Operator will be provided the right to inspect Escrow Agent's applicable records upon reasonable prior notice and during normal business hours. Registry Operator and ICANN will be provided with the right to designate a third-party auditor to audit Escrow Agent's compliance with the technical specifications and maintenance requirements of this Specification 2 from time to time.

    If Escrow Agent receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposits, Escrow Agent will promptly notify the Registry Operator and ICANN unless prohibited by law. After notifying the Registry Operator and ICANN, Escrow Agent shall allow

sufficient time for Registry Operator or ICANN to challenge any such order, which shall be the responsibility of Registry Operator or ICANN; provided, however, that Escrow Agent does not waive its rights to present its position with respect to any such order. Escrow Agent will cooperate with the Registry Operator or ICANN to support efforts to quash or limit any subpoena, at such party's expense. Any party requesting additional assistance shall pay Escrow Agent's standard charges or as quoted upon submission of a detailed request.

5. **Copies**. Escrow Agent may be permitted to duplicate any Deposit, in order to comply with the terms and provisions of the escrow agreement.

6. **Release of Deposits**. Escrow Agent will make available for electronic download (unless otherwise requested) to ICANN or its designee, within twenty-four (24) hours, at the Registry Operator's expense, all Deposits in Escrow Agent's possession in the event that the Escrow Agent receives a request from Registry Operator to effect such delivery to ICANN, or receives one of the following written notices by ICANN stating that:

6.1. the Registry Agreement has expired without renewal, or been terminated; or

6.2. ICANN has not received a notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent within five (5) calendar days after the Deposit's scheduled delivery date; (a) ICANN gave notice to Escrow Agent and Registry Operator of that failure; and (b) ICANN has not, within seven (7) calendar days after such notice, received the notification from Escrow Agent; or

6.3. ICANN has received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of failed verification of the latest escrow deposit for a specific date or a notification of a missing deposit, and the notification is for a deposit that should have been made on Sunday (i.e., a Full Deposit); (a) ICANN gave notice to Registry Operator of that receipt; and (b) ICANN has not, within seven (7) calendar days after such notice, received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of verification of a remediated version of such Full Deposit; or

6.4. ICANN has received five notifications from Escrow Agent within the last thirty (30) calendar days notifying ICANN of either missing or failed escrow deposits that should have been made Monday through Saturday (i.e., a Differential Deposit), and (x) ICANN provided notice to Registry Operator of the receipt of such notifications; and (y) ICANN has not, within seven (7) calendar days after delivery of such notice to Registry Operator, received notification from Escrow Agent of verification of a remediated version of such Differential Deposit; or

6.5. Registry Operator has: (i) ceased to conduct its business in the ordinary course; or (ii) filed for bankruptcy, become insolvent or anything analogous to any of the foregoing under the laws of any jurisdiction anywhere in the world; or

6.6. Registry Operator has experienced a failure of critical registry functions and ICANN has asserted its rights pursuant to Section 2.13 of the Agreement; or

6.7. a competent court, arbitral, legislative, or government agency mandates the release of the Deposits to ICANN; or

6.8. pursuant to Contractual and Operational Compliance Audits as specified under Section 2.11 of the Agreement.

Unless Escrow Agent has previously released the Registry Operator's Deposits to ICANN or its designee, Escrow Agent will deliver all Deposits to ICANN upon expiration or termination of the Registry Agreement or the Escrow Agreement.

7. **Verification of Deposits**.

7.1. Within twenty-four (24) hours after receiving each Deposit or corrected Deposit, Escrow Agent must verify the format and completeness of each Deposit and deliver to ICANN a notification generated for each Deposit. Reports will be delivered electronically using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification.

7.2. If Escrow Agent discovers that any Deposit fails the verification procedures or if Escrow Agent does not receive any scheduled Deposit, Escrow Agent must notify Registry Operator either by email, fax or phone and ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Part A, Section 9, reference 5 of this Specification) of such nonconformity or non-receipt within twenty-four (24) hours after receiving the non-conformant Deposit or the deadline for such Deposit, as applicable. Upon notification of such verification or delivery failure, Registry Operator must begin developing modifications, updates, corrections, and other fixes of the Deposit necessary for the Deposit to be delivered and pass the verification procedures and deliver such fixes to Escrow Agent as promptly as possible.

8. **Amendments**. Escrow Agent and Registry Operator shall amend the terms of the Escrow Agreement to conform to this Specification 2 within ten (10) calendar days of any amendment or modification to this Specification 2. In the event of a conflict between this Specification 2 and the Escrow Agreement, this Specification 2 shall control.

9. **Indemnity**. Escrow Agent shall indemnify and hold harmless Registry Operator and ICANN, and each of their respective directors, officers, agents, employees, members,

and stockholders ("Indemnitees") absolutely and forever from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorneys' fees and costs, that may be asserted by a third party against any Indemnitee in connection with the misrepresentation, negligence or misconduct of Escrow Agent, its directors, officers, agents, employees and contractors.

SPECIFICATION 3

FORMAT AND CONTENT FOR REGISTRY OPERATOR MONTHLY REPORTING

Registry Operator shall provide one set of monthly reports per gTLD, using the API described in draft-lozano-icann-registry-interfaces, see Specification 2, Part A, Section 9, reference 5, with the following content.

ICANN may request in the future that the reports be delivered by other means and using other formats. ICANN will use reasonable commercial efforts to preserve the confidentiality of the information reported until three (3) months after the end of the month to which the reports relate. Unless set forth in this Specification 3, any reference to a specific time refers to Coordinated Universal Time (UTC). Monthly reports shall consist of data that reflects the state of the registry at the end of the month (UTC).

1. **Per-Registrar Transactions Report**. This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD-transactions-yyyymm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyymm" is the year and month being reported. The file shall contain the following fields per registrar:

Field #	Field name	Description
01	registrar-name	Registrar's full corporate name as registered with IANA
02	iana-id	For cases where the registry operator acts as registrar (i.e., without the use of an ICANN accredited registrar) 9999 should be used, otherwise the sponsoring Registrar IANA id should be used as specified in http://www.iana.org/assignments/registrar-ids
03	total-domains	total domain names under sponsorship in any EPP status but pendingCreate that have not been purged
04	total-nameservers	total name servers (either host objects or name server hosts as domain name attributes) associated with domain names registered for the TLD in any EPP status but pendingCreate that have not been purged
05	net-adds-1-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of one (1) year (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
06	net-adds-2-yr	number of domains successfully registered (i.e., not

		in EPP pendingCreate status) with an initial term of two(2) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
07	net-adds-3-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of three (3) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
08	net-adds-4-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of four (4) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
09	net-adds-5-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of five (5) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
10	net-adds-6-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of six (6) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
11	net-adds-7-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of seven (7) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
12	net-adds-8-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of eight (8) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
13	net-adds-9-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of nine (9) years (and not deleted within the add grace period). A transaction must be reported in the month the add grace period ends.
14	net-adds-10-yr	number of domains successfully registered (i.e., not in EPP pendingCreate status) with an initial term of ten (10) years (and not deleted within the add grace period). A transaction must be reported in the month

		the add grace period ends.
15	net-renews-1-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of one (1) year (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
16	net-renews-2-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of two (2) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
17	net-renews-3-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of three (3) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
18	net-renews-4-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of four (4) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
19	net-renews-5-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of five (5) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
20	net-renews-6-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of six (6) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.

21	net-renews-7-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of seven (7) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
22	net-renews-8-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of eight (8) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
23	net-renews-9-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of nine (9) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
24	net-renews-10-yr	number of domains successfully renewed (i.e., not in EPP pendingRenew status) either automatically or by command with a new renewal period of ten (10) years (and not deleted within the renew or auto-renew grace period). A transaction must be reported in the month the renew or auto-renew grace period ends.
25	transfer-gaining-successful	number of domain transfers initiated by this registrar that were successfully completed (either explicitly or automatically approved) and not deleted within the transfer grace period. A transaction must be reported in the month the transfer grace period ends.
26	transfer-gaining-nacked	number of domain transfers initiated by this registrar that were rejected (e.g., EPP transfer op="reject") by the other registrar
27	transfer-losing-successfully	number of domain transfers initiated by another registrar that were successfully completed (either explicitly or automatically approved)
28	transfer-losing-nacked	number of domain transfers initiated by another registrar that this registrar rejected (e.g., EPP transfer op="reject")

29	transfer-disputed-won	number of transfer disputes in which this registrar prevailed (reported in the month where the determination happened)
30	transfer-disputed-lost	number of transfer disputes this registrar lost (reported in the month where the determination happened)
31	transfer-disputed-nodecision	number of transfer disputes involving this registrar with a split or no decision (reported in the month where the determination happened)
32	deleted-domains-grace	domains deleted within the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
33	deleted-domains-nograce	domains deleted outside the add grace period (does not include names deleted while in EPP pendingCreate status). A deletion must be reported in the month the name is purged.
34	restored-domains	domain names restored from redemption period
35	restored-noreport	total number of restored names for which the registrar failed to submit a restore report
36	agp-exemption-requests	total number of AGP (add grace period) exemption requests
37	agp-exemptions-granted	total number of AGP (add grace period) exemption requests granted
38	agp-exempted-domains	total number of names affected by granted AGP (add grace period) exemption requests
39	attempted-adds	number of attempted (both successful and failed) domain name create commands

The first line shall include the field names exactly as described in the table above as a "header line" as described in section 2 of RFC 4180. The last line of each report shall include totals for each column across all registrars; the first field of this line shall read "Totals" while the second field shall be left empty in that line. No other lines besides the ones described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

2.   **Registry Functions Activity Report**. This report shall be compiled in a comma separated-value formatted file as specified in RFC 4180. The file shall be named "gTLD-activity-yyyymm.csv", where "gTLD" is the gTLD name; in case of an IDN-TLD, the A-label shall be used; "yyyymm" is the year and month being reported. The file shall contain the following fields:

Field #	Field Name	Description
01	operational-registrars	number of operational registrars at the end of the reporting period
02	ramp-up-registrars	number of registrars that have received a password for access to OT&E at the end of the reporting period
03	pre-ramp-up-registrars	number of registrars that have requested access, but have not yet entered the ramp-up period at the end of the reporting period
04	zfa-passwords	number of active zone file access passwords at the end of the reporting period
05	whois-43-queries	number of WHOIS (port-43) queries responded during the reporting period
06	web-whois-queries	number of Web-based Whois queries responded during the reporting period, not including searchable Whois
07	searchable-whois-queries	number of searchable Whois queries responded during the reporting period, if offered
08	dns-udp-queries-received	number of DNS queries received over UDP transport during the reporting period
09	dns-udp-queries-responded	number of DNS queries received over UDP transport that were responded during the reporting period
10	dns-tcp-queries-received	number of DNS queries received over TCP transport during the reporting period
11	dns-tcp-queries-responded	number of DNS queries received over TCP transport that were responded during the reporting period
12	srs-dom-check	number of SRS (EPP and any other interface) domain name "check" requests responded during the reporting period
13	srs-dom-create	number of SRS (EPP and any other interface) domain name "create" requests responded during the reporting period
14	srs-dom-delete	number of SRS (EPP and any other interface) domain name "delete" requests responded during the reporting period
15	srs-dom-info	number of SRS (EPP and any other interface) domain name "info" requests responded during the reporting period

Field #	Field Name	Description
16	srs-dom-renew	number of SRS (EPP and any other interface) domain name "renew" requests responded during the reporting period
17	srs-dom-rgp-restore-report	number of SRS (EPP and any other interface) domain name RGP "restore" requests delivering a restore report responded during the reporting period
18	srs-dom-rgp-restore-request	number of SRS (EPP and any other interface) domain name RGP "restore" requests responded during the reporting period
19	srs-dom-transfer-approve	number of SRS (EPP and any other interface) domain name "transfer" requests to approve transfers responded during the reporting period
20	srs-dom-transfer-cancel	number of SRS (EPP and any other interface) domain name "transfer" requests to cancel transfers responded during the reporting period
21	srs-dom-transfer-query	number of SRS (EPP and any other interface) domain name "transfer" requests to query about a transfer responded during the reporting period
22	srs-dom-transfer-reject	number of SRS (EPP and any other interface) domain name "transfer" requests to reject transfers responded during the reporting period
23	srs-dom-transfer-request	number of SRS (EPP and any other interface) domain name "transfer" requests to request transfers responded during the reporting period
24	srs-dom-update	number of SRS (EPP and any other interface) domain name "update" requests (not including RGP restore requests) responded during the reporting period
25	srs-host-check	number of SRS (EPP and any other interface) host "check" requests responded during the reporting period
26	srs-host-create	number of SRS (EPP and any other interface) host "create" requests responded during the reporting period
27	srs-host-delete	number of SRS (EPP and any other interface) host "delete" requests responded during the reporting period

Field #	Field Name	Description
28	srs-host-info	number of SRS (EPP and any other interface) host "info" requests responded during the reporting period
29	srs-host-update	number of SRS (EPP and any other interface) host "update" requests responded during the reporting period
30	srs-cont-check	number of SRS (EPP and any other interface) contact "check" requests responded during the reporting period
31	srs-cont-create	number of SRS (EPP and any other interface) contact "create" requests responded during the reporting period
32	srs-cont-delete	number of SRS (EPP and any other interface) contact "delete" requests responded during the reporting period
33	srs-cont-info	number of SRS (EPP and any other interface) contact "info" requests responded during the reporting period
34	srs-cont-transfer-approve	number of SRS (EPP and any other interface) contact "transfer" requests to approve transfers responded during the reporting period
35	srs-cont-transfer-cancel	number of SRS (EPP and any other interface) contact "transfer" requests to cancel transfers responded during the reporting period
36	srs-cont-transfer-query	number of SRS (EPP and any other interface) contact "transfer" requests to query about a transfer responded during the reporting period
37	srs-cont-transfer-reject	number of SRS (EPP and any other interface) contact "transfer" requests to reject transfers responded during the reporting period
38	srs-cont-transfer-request	number of SRS (EPP and any other interface) contact "transfer" requests to request transfers responded during the reporting period
39	srs-cont-update	number of SRS (EPP and any other interface) contact "update" requests responded during the reporting period

The first line shall include the field names exactly as described in the table above as a "header line" as described in section 2 of RFC 4180. No other lines besides the ones

described above shall be included. Line breaks shall be <U+000D, U+000A> as described in RFC 4180.

For gTLDs that are part of a single-instance Shared Registry System, the Registry Functions Activity Report may include the total contact or host transactions for all the gTLDs in the system.

SPECIFICATION 4

REGISTRATION DATA PUBLICATION SERVICES

1. **Registration Data Directory Services**. Until ICANN requires a different protocol, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at <whois.nic.TLD> providing free public query-based access to at least the following elements in the following format. ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable.

   Registry Operator shall implement a new standard supporting access to domain name registration data (SAC 051) no later than one hundred thirty-five (135) days after it is requested by ICANN if: 1) the IETF produces a standard (i.e., it is published, at least, as a Proposed Standard RFC as specified in RFC 2026); and 2) its implementation is commercially reasonable in the context of the overall operation of the registry.

   1.1.   The format of responses shall follow a semi-free text format outline below, followed by a blank line and a legal disclaimer specifying the rights of Registry Operator, and of the user querying the database.

   1.2.   Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.

   1.3.   For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

   1.4.   The fields specified below set forth the minimum output requirements. Registry Operator may output data fields in addition to those specified below, subject to approval by ICANN, which approval shall not be unreasonably withheld.

   1.5.   **Domain Name Data:**

      1.5.1   **Query format:** whois EXAMPLE.TLD

      1.5.2   **Response format:**

      Domain Name: EXAMPLE.TLD
      Domain ID: D1234567-TLD

WHOIS Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD
Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234

Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.6. **Registrar Data:**

1.6.1 **Query format**: whois "registrar Example Registrar, Inc."

1.6.2 **Response format**:

Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.tld
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
Admin Contact: Joe Registrar
Phone Number: +1.3105551213
Fax Number: +1.3105551213
Email: joeregistrar@example-registrar.tld
Admin Contact: Jane Registrar
Phone Number: +1.3105551214
Fax Number: +1.3105551213
Email: janeregistrar@example-registrar.tld
Technical Contact: John Geek
Phone Number: +1.3105551215
Fax Number: +1.3105551216
Email: johngeek@example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.7. **Nameserver Data:**

1.7.1 **Query format**: whois "NS1.EXAMPLE.TLD", whois "nameserver (nameserver name)", or whois "nameserver (IP Address)"

1.7.2 **Response format:**

Server Name: NS1.EXAMPLE.TLD
IP Address: 192.0.2.123 IP
Address: 2001:0DB8::1
Registrar: Example Registrar, Inc.
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
\>\>\> Last update of WHOIS database: 2009-05-29T20:15:00Z \<\<\<

1.8.   The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers (the extension will be provided as a separate field as shown above), email addresses, date and times should conform to the mappings specified in EPP RFCs 5730-5734 so that the display of this information (or values return in WHOIS responses) can be uniformly processed and understood.

1.9.   In order to be compatible with ICANN's common interface for WHOIS (InterNIC), WHOIS output shall be in the format outline above.

1.10. **Searchability**. Offering searchability capabilities on the Directory Services is optional but if offered by the Registry Operator it shall comply with the specification described in this section.

   1.10.1 Registry Operator will offer searchability on the web-based Directory Service.

   1.10.2 Registry Operator will offer partial match capabilities, at least, on the following fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.).

   1.10.3 Registry Operator will offer exact-match capabilities, at least, on the following fields: registrar id, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records).

   1.10.4 Registry Operator will offer Boolean search capabilities supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT.

   1.10.5 Search results will include domain names matching the search criteria.

   1.10.6 Registry Operator will: 1) implement appropriate measures to avoid abuse of this feature (e.g., permitting access only to legitimate authorized users); and 2) ensure the feature is in compliance with any applicable privacy laws or policies.

1.11. Registry Operator shall provide a link on the primary website for the TLD (i.e., the website provided to ICANN for publishing on the ICANN website) to a web page designated by ICANN containing WHOIS policy and educational materials.

2. **Zone File Access**

2.1. **Third-Party Access**

2.1.1 **Zone File Access Agreement**. Registry Operator will enter into an agreement with any Internet user, which will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider, which may be ICANN or an ICANN designee (the "CZDA Provider"). Registry Operator (optionally through the CZDA Provider) will provide access to zone file data per Section 2.1.3 of this Specification and do so using the file format described in Section 2.1.4 of this Specification. Notwithstanding the foregoing, (a) the CZDA Provider may reject the request for access of any user that does not satisfy the credentialing requirements in Section 2.1.2 below; (b) Registry Operator may reject the request for access of any user that does not provide correct or legitimate credentials under Section 2.1.2 below or where Registry Operator reasonably believes will violate the terms of Section 2.1.5. below; and, (c) Registry Operator may revoke access of any user if Registry Operator has evidence to support that the user has violated the terms of Section 2.1.5 below.

2.1.2 **Credentialing Requirements**. Registry Operator, through the facilitation of the CZDA Provider, will request each user to provide it with information sufficient to correctly identify and locate the user. Such user information will include, without limitation, company name, contact name, address, telephone number, facsimile number, email address and IP address.

2.1.3 **Grant of Access**. Each Registry Operator (optionally through the CZDA Provider) will provide the Zone File FTP (or other Registry supported) service for an ICANN-specified and managed URL (specifically, <TLD>.zda.icann.org where <TLD> is the TLD for which the registry is responsible) for the user to access the Registry's zone data archives. Registry Operator will grant the user a non-exclusive, nontransferable, limited right to access Registry Operator's (optionally CZDA Provider's) Zone File hosting server, and to transfer a copy of the top-level domain zone files, and any associated cryptographic checksum files no more than once per 24 hour period using FTP, or other data transport and access protocols that may be

prescribed by ICANN. For every zone file access server, the zone files are in the top-level directory called <zone>.zone.gz, with <zone>.zone.gz.md5 and <zone>.zone.gz.sig to verify downloads. If the Registry Operator (or the CZDA Provider) also provides historical data, it will use the naming pattern <zone>-yyyymmdd.zone.gz, etc.

2.1.4 **File Format Standard**. Registry Operator (optionally through the CZDA Provider) will provide zone files using a subformat of the standard Master File format as originally defined in RFC 1035, Section 5, including all the records present in the actual zone used in the public DNS. Sub-format is as follows:

1. Each record must include all fields in one line as: <domain-name> <TTL> <class> <type> <RDATA>.

2. Class and Type must use the standard mnemonics and must be in lower case.

3. TTL must be present as a decimal integer.

4. Use of /X and /DDD inside domain names is allowed.

5. All domain names must be in lower case.

6. Must use exactly one tab as separator of fields inside a record.

7. All domain names must be fully qualified.

8. No $ORIGIN directives.

9. No use of "@" to denote current origin.

10. No use of "blank domain names" at the beginning of a record to continue the use of the domain name in the previous record.

11. No $INCLUDE directives.

12. No $TTL directives.

13. No use of parentheses, e.g., to continue the list of fields in a record across a line boundary.

14. No use of comments.

15. No blank lines.

16. The SOA record should be present at the top and (duplicated at) the end of the zone file.

17. With the exception of the SOA record, all the records in a file must be in alphabetical order.

18. One zone per file. If a TLD divides its DNS data into multiple zones, each goes into a separate file named as above, with all the files combined using tar into a file called <tld>.zone.tar.

    2.1.5 **Use of Data by User**. Registry Operator will permit user to use the zone file for lawful purposes; provided that (a) user takes all reasonable steps to protect against unauthorized access to and use and disclosure of the data and (b) under no circumstances will Registry Operator be required or permitted to allow user to use the data to, (i) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar.

    2.1.6 **Term of Use**. Registry Operator, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months. Registry Operator will allow users to renew their Grant of Access.

    2.1.7 **No Fee for Access**. Registry Operator will provide, and CZDA Provider will facilitate, access to the zone file to user at no cost.

2.2. **Co-operation**

    2.2.1 **Assistance**. Registry Operator will co-operate and provide reasonable assistance to ICANN and the CZDA Provider to facilitate and maintain the efficient access of zone file data by permitted users as contemplated under this Schedule.

2.3. **ICANN Access**. Registry Operator shall provide bulk access to the zone files for the TLD to ICANN or its designee on a continuous basis in the manner ICANN may reasonably specify from time to time. Access will be provided at least daily. Zone files will include SRS data committed as close as possible to 00:00:00 UTC.

2.4. **Emergency Operator Access**. Registry Operator shall provide bulk access to the zone files for the TLD to the Emergency Operators designated by ICANN on a continuous basis in the manner ICANN may reasonably specify from time to time.

3. **Bulk Registration Data Access to ICANN**

3.1. **Periodic Access to Thin Registration Data**. In order to verify and ensure the operational stability of Registry Services as well as to facilitate compliance checks on accredited registrars, Registry Operator will provide ICANN on a weekly basis (the day to be designated by ICANN) with up-to-date Registration Data as specified below. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.

    3.1.1 **Contents**. Registry Operator will provide, at least, the following data for all registered domain names: domain name, domain name repository object id (roid), registrar id (IANA ID), statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, at least, it will provide: registrar name, registrar repository object id (roid), hostname of registrar Whois server, and URL of registrar.

    3.1.2 **Format**. The data will be provided in the format specified in Specification 2 for Data Escrow (including encryption, signing, etc.) but including only the fields mentioned in the previous section, i.e., the file will only contain Domain and Registrar objects with the fields mentioned above. Registry Operator has the option to provide a full deposit file instead as specified in Specification 2.

    3.1.3 **Access**. Registry Operator will have the file(s) ready for download as of 00:00:00 UTC on the day designated for retrieval by ICANN. The file(s) will be made available for download by SFTP, though ICANN may request other means in the future.

3.2. **Exceptional Access to Thick Registration Data**. In case of a registrar failure, deaccreditation, court order, etc. that prompts the temporary or definitive transfer of its domain names to another registrar, at the request of ICANN, Registry Operator will provide ICANN with up-to-date data for the domain names of the losing registrar. The data will be provided in the format specified in Specification 2 for Data Escrow. The file will only contain data related to the domain names of the losing registrar. Registry Operator will provide the data as soon as commercially practicable, but in no event later than five (5) calendar days following ICANN's request. Unless otherwise agreed by Registry Operator and ICANN, the file will be made available for download by ICANN in the same manner as the data specified in Section 3.1 of this Specification.

SPECIFICATION 5

SCHEDULE OF RESERVED NAMES

Except to the extent that ICANN otherwise expressly authorizes in writing, and subject to the terms and conditions of this Specification, Registry Operator shall reserve the following labels from initial (i.e., other than renewal) registration within the TLD. If using self-allocation, the Registry Operator must show the registration in the RDDS. In the case of IDN names (as indicated below), IDN variants will be identified according to the registry operator IDN registration policy, where applicable.

1. **Example.** The ASCII label "EXAMPLE" shall be withheld from registration or allocated to Registry Operator at the second level and at all other levels within the TLD at which Registry Operator offers registrations (such second level and all other levels are collectively referred to herein as, "All Levels"). Such label may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, such withheld or allocated label shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such name without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

2. **Two-character labels**. All two-character ASCII labels shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Such labels may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator, provided that such two-character label strings may be released to the extent that Registry Operator reaches agreement with the related government and country-code manager of the string as specified in the ISO 3166-1 alpha-2 standard. The Registry Operator may also propose the release of these reservations based on its implementation of measures to avoid confusion with the corresponding country codes, subject to approval by ICANN. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such labels that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

3. **Reservations for Registry Operations**.

    3.1. The following ASCII labels must be withheld from registration or allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: WWW, RDDS and WHOIS. The following ASCII label must be allocated to Registry Operator at All Levels for use in connection with the operation of the registry for the TLD: NIC. Registry Operator may activate WWW, RDDS and WHOIS in the DNS, but must activate NIC in the

DNS, as necessary for the operation of the TLD. None of WWW, RDDS, WHOIS or NIC may be released or registered to any person (other than Registry Operator) or third party. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD all such withheld or allocated names shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

3.2. Registry Operator may activate in the DNS at All Levels up to one hundred (100) names (plus their IDN variants, where applicable) necessary for the operation or the promotion of the TLD. Registry Operator must act as the Registered Name Holder of such names as that term is defined in the then-current ICANN Registrar Accreditation Agreement (RAA). These activations will be considered Transactions for purposes of Section 6.1 of the Agreement. Registry Operator must either (i) register such names through an ICANN-accredited registrar; or (ii) self-allocate such names and with respect to those names submit to and be responsible to ICANN for compliance with ICANN Consensus Policies and the obligations set forth in Subsections 3.7.7.1 through 3.7.7.12 of the then-current RAA (or any other replacement clause setting out the terms of the registration agreement between a registrar and a registered name holder). At Registry Operator's discretion and in compliance with all other terms of this Agreement, such names may be released for registration to another person or entity.

3.3. Registry Operator may withhold from registration or allocate to Registry Operator names (including their IDN variants, where applicable) at All Levels in accordance with Section 2.6 of the Agreement. Such names may not be activated in the DNS, but may be released for registration to another person or entity at Registry Operator's discretion. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Upon ICANN's request, Registry Operator shall provide a listing of all names withheld or allocated to Registry Operator pursuant to Section 2.6 of the Agreement. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

4. **Country and Territory Names**. The country and territory names (including their IDN variants, where applicable) contained in the following internationally recognized lists shall be withheld from registration or allocated to Registry Operator at All Levels:

4.1. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European

Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union <http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm>;

4.2. the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and

4.3. the list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names;

provided, that the reservation of specific country and territory names (including their IDN variants according to the registry operator IDN registration policy, where applicable) may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry Operator must not activate such names in the DNS; provided, that Registry Operator may propose the release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names that remain withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

5. **International Olympic Committee; International Red Cross and Red Crescent Movement**. As instructed from time to time by ICANN, the names (including their IDN variants, where applicable) relating to the International Olympic Committee, International Red Cross and Red Crescent Movement listed at http://www.icann.org/en/resources/registries/reserved shall be withheld from registration or allocated to Registry Operator at the second level within the TLD. Additional International Olympic Committee, International Red Cross and Red Crescent Movement names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Such names may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such names withheld from registration or allocated to Registry Operator shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

6. **Intergovernmental Organizations**. As instructed from time to time by ICANN, Registry Operator will implement the protections mechanism determined by the

ICANN Board of Directors relating to the protection of identifiers for Intergovernmental Organizations. A list of reserved names for this Section 6 is available at http://www.icann.org/en/resources/registries/reserved. Additional names (including their IDN variants) may be added to the list upon ten (10) calendar days notice from ICANN to Registry Operator. Any such protected identifiers for Intergovernmental Organizations may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator. Upon conclusion of Registry Operator's designation as operator of the registry for the TLD, all such protected identifiers shall be transferred as specified by ICANN. Registry Operator may self-allocate and renew such names without use of an ICANN accredited registrar, which will not be considered Transactions for purposes of Section 6.1 of the Agreement.

SPECIFICATION 6

REGISTRY INTEROPERABILITY AND CONTINUITY SPECIFICATIONS

1. **Standards Compliance**

    1.1. **DNS**. Registry Operator shall comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF), including all successor standards, modifications or additions thereto relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343, and 5966. DNS labels may only include hyphens in the third and fourth position if they represent valid IDNs (as specified above) in their ASCII encoding (e.g., "xn--ndk061n").

    1.2. **EPP**. Registry Operator shall comply with relevant existing RFCs and those published in the future by the Internet Engineering Task Force (IETF) including all successor standards, modifications or additions thereto relating to the provisioning and management of domain names using the Extensible Provisioning Protocol (EPP) in conformance with RFCs 5910, 5730, 5731, 5732 (if using host objects), 5733 and 5734. If Registry Operator implements Registry Grace Period (RGP), it will comply with RFC 3915 and its successors. If Registry Operator requires the use of functionality outside the base EPP RFCs, Registry Operator must document EPP extensions in Internet-Draft format following the guidelines described in RFC 3735. Registry Operator will provide and update the relevant documentation of all the EPP Objects and Extensions supported to ICANN prior to deployment.

    1.3. **DNSSEC**. Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions ("DNSSEC"). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 and their successors, and follow the best practices described in RFC 4641 and its successors. If Registry Operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors. Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices. Registry shall also publish in its website the DNSSEC Practice Statements (DPS) describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material. Registry Operator shall publish its DPS following the format described in RFC 6841.

    1.4. **IDN**. If the Registry Operator offers Internationalized Domain Names ("IDNs"), it shall comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registry Operator shall comply with the ICANN IDN Guidelines at <http://www.icann.org/en/topics/idn/implementation-guidelines.htm>,

as they may be amended, modified, or superseded from time to time. Registry Operator shall publish and keep updated its IDN Tables and IDN Registration Rules in the IANA Repository of IDN Practices as specified in the ICANN IDN Guidelines.

1.5. **IPv6**. Registry Operator shall be able to accept IPv6 addresses as glue records in its Registry System and publish them in the DNS. Registry Operator shall offer public IPv6 transport for, at least, two of the Registry's name servers listed in the root zone with the corresponding IPv6 addresses registered with IANA. Registry Operator should follow "DNS IPv6 Transport Operational Guidelines" as described in BCP 91 and the recommendations and considerations described in RFC 4472. Registry Operator shall offer public IPv6 transport for its Registration Data Publication Services as defined in Specification 4 of this Agreement; e.g., Whois (RFC 3912), Web based Whois. Registry Operator shall offer public IPv6 transport for its Shared Registration System (SRS) to any Registrar, no later than six (6) months after receiving the first request in writing from a gTLD accredited Registrar willing to operate with the SRS over IPv6.

2. **Registry Services**

2.1. **Registry Services**. "Registry Services" are, for purposes of the Agreement, defined as the following: (a) those services that are operations of the registry critical to the following tasks: the receipt of data from registrars concerning registrations of domain names and name servers; provision to registrars of status information relating to the zone servers for the TLD; dissemination of TLD zone files; operation of the registry DNS servers; and dissemination of contact and other information concerning domain name server registrations in the TLD as required by this Agreement; (b) other products or services that the Registry Operator is required to provide because of the establishment of a Consensus Policy as defined in Specification 1; (c) any other products or services that only a registry operator is capable of providing, by reason of its designation as the registry operator; and (d) material changes to any Registry Service within the scope of (a), (b) or (c) above.

2.2. **Wildcard Prohibition**. For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFCs 1034 and 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry

Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

3. **Registry Continuity**

    3.1. **High Availability**. Registry Operator will conduct its operations using network and geographically diverse, redundant servers (including network-level redundancy, end-node level redundancy and the implementation of a load balancing scheme where applicable) to ensure continued operation in the case of technical failure (widespread or local), or an extraordinary occurrence or circumstance beyond the control of the Registry Operator.

    3.2. **Extraordinary Event**. Registry Operator will use commercially reasonable efforts to restore the critical functions of the registry within twenty-four (24) hours after the termination of an extraordinary event beyond the control of the Registry Operator and restore full system functionality within a maximum of forty-eight (48) hours following such event, depending on the type of critical function involved. Outages due to such an event will not be considered a lack of service availability.

    3.3. **Business Continuity**. Registry Operator shall maintain a business continuity plan, which will provide for the maintenance of Registry Services in the event of an extraordinary event beyond the control of the Registry Operator or business failure of Registry Operator, and may include the designation of a Registry Services continuity provider. If such plan includes the designation of a Registry Services continuity provider, Registry Operator shall provide the name and contact information for such Registry Services continuity provider to ICANN. In the case of an extraordinary event beyond the control of the Registry Operator where the Registry Operator cannot be contacted, Registry Operator consents that ICANN may contact the designated Registry Services continuity provider, if one exists. Registry Operator shall conduct Registry Services Continuity testing at least once per year.

4. **Abuse Mitigation**

    4.1. **Abuse Contact**. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquires related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.

    4.2. **Malicious Use of Orphan Glue Records**. Registry Operator shall take action to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

5.   **Supported Initial and Renewal Registration Periods**

    5.1.   **Initial Registration Periods**. Initial registrations of registered names may be made in the registry in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, initial registrations of registered names may not exceed ten (10) years.

    5.2.   **Renewal Periods**. Renewal of registered names may be made in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, renewal of registered names may not extend their registration period beyond ten (10) years from the time of the renewal.

SPECIFICATION 7

MINIMUM REQUIREMENTS FOR RIGHTS PROTECTION MECHANISMS

1.   **Rights Protection Mechanisms**. Registry Operator shall implement and adhere to the rights protection mechanisms ("RPMs") specified in this Specification. In addition to such RPMs, Registry Operator may develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party's legal rights. Registry Operator will include all RPMs required by this Specification 7 and any additional RPMs developed and implemented by Registry Operator in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD. Registry Operator shall implement in accordance with requirements set forth therein each of the mandatory RPMs set forth in the Trademark Clearinghouse as of the date hereof, as posted at [*url to be inserted*] (the "Trademark Clearinghouse Requirements"), which may be revised in immaterial respects by ICANN from time to time. Registry Operator shall not mandate that any owner of applicable intellectual property rights use any other trademark information aggregation, notification, or validation service in addition to or instead of the ICANN-designated Trademark Clearinghouse. If there is a conflict between the terms and conditions of this Agreement and the Trademark Clearinghouse Requirements, the terms and conditions of this Agreement shall control.

2.   **Dispute Resolution Mechanisms**. Registry Operator will comply with the following dispute resolution mechanisms as they may be revised from time to time:

   a.   the Trademark Post-Delegation Dispute Resolution Procedure (PDDRP) and the Registration Restriction Dispute Resolution Procedure (RRDRP) adopted by ICANN (posted at [urls to be inserted when final procedure is adopted]). Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PDDRP or RRDRP panel and to be bound by any such determination; and

   b.   the Uniform Rapid Suspension system ("URS") adopted by ICANN (posted at [url to be inserted]), including the implementation of determinations issued by URS examiners.

SPECIFICATION 8

CONTINUED OPERATIONS INSTRUMENT

1. The Continued Operations Instrument shall (a) provide for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6th) anniversary of the Effective Date, and (b) be in the form of either (i) an irrevocable standby letter of credit, or (ii) an irrevocable cash escrow deposit, each meeting the requirements set forth in item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof (which is hereby incorporated by reference into this Specification 8). Registry Operator shall use its best efforts to take all actions necessary or advisable to maintain in effect the Continued Operations Instrument for a period of six (6) years from the Effective Date, and to maintain ICANN as a third party beneficiary thereof. If Registry Operator elects to obtain an irrevocable standby letter of credit but the term required above is unobtainable, Registry Operator may obtain a letter of credit with a one-year term and an "evergreen provision," providing for annual extensions, without amendment, for an indefinite number of additional periods until the issuing bank informs ICANN of its final expiration or until ICANN releases the letter of credit as evidenced in writing, if the letter of credit otherwise meets the requirements set forth in item 50(b) of Attachment to Module 2 – Evaluation Questions and Criteria – of the gTLD Applicant Guidebook, as published and supplemented by ICANN prior to the date hereof; provided, however, that if the issuing bank informs ICANN of the expiration of such letter of credit prior to the sixth (6th) anniversary of the Effective Date, such letter of credit must provide that ICANN is entitled to draw the funds secured by the letter of credit prior to such expiration. The letter of credit must require the issuing bank to give ICANN at least thirty (30) calendar days' notice of any such expiration or non-renewal. If the letter of credit expires or is terminated at any time prior to the sixth (6th) anniversary of the Effective Date, Registry Operator will be required to obtain a replacement Continued Operations Instrument. ICANN may draw the funds under the original letter of credit, if the replacement Continued Operations Instrument is not in place prior to the expiration of the original letter of credit. Registry Operator shall provide to ICANN copies of all final documents relating to the Continued Operations Instrument and shall keep ICANN reasonably informed of material developments relating to the Continued Operations Instrument. Registry Operator shall not agree to, or permit, any amendment of, or waiver under, the Continued Operations Instrument or other documentation relating thereto without the prior written consent of ICANN (such consent not to be unreasonably withheld).

2.	If, notwithstanding the use of best efforts by Registry Operator to satisfy its obligations under the preceding paragraph, the Continued Operations Instrument expires or is terminated by another party thereto, in whole or in part, for any reason, prior to the sixth anniversary of the Effective Date, Registry Operator shall promptly (i) notify ICANN of such expiration or termination and the reasons therefor and (ii) arrange for an alternative instrument that provides for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period of one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) anniversary of the Effective Date (an "Alternative Instrument"). Any such Alternative Instrument shall be on terms no less favorable to ICANN than the Continued Operations Instrument and shall otherwise be in form and substance reasonably acceptable to ICANN.

3.	Notwithstanding anything to the contrary contained in this Specification 8, at any time, Registry Operator may replace the Continued Operations Instrument with an Alternative Instrument that (i) provides for sufficient financial resources to ensure the continued operation of the critical registry functions related to the TLD set forth in Section 6 of Specification 10 to this Agreement for a period of three (3) years following any termination of this Agreement on or prior to the fifth anniversary of the Effective Date or for a period one (1) year following any termination of this Agreement after the fifth anniversary of the Effective Date but prior to or on the sixth (6) anniversary of the Effective Date, and (ii) contains terms no less favorable to ICANN than the Continued Operations Instrument and is otherwise in form and substance reasonably acceptable to ICANN. In the event Registry Operator replaces the Continued Operations Instrument either pursuant to paragraph 2 or this paragraph 3, the terms of this Specification 8 shall no longer apply with respect to the original Continuing Operations Instrument, but shall thereafter apply with respect to such Alternative Instrument(s), and such instrument shall thereafter be considered the Continued Operations Instrument for purposes of this Agreement.

SPECIFICATION 9

REGISTRY OPERATOR CODE OF CONDUCT

1. In connection with the operation of the registry for the TLD, Registry Operator will not, and will not allow any parent, subsidiary, Affiliate, subcontractor or other related entity, to the extent such party is engaged in the provision of Registry Services with respect to the TLD (each, a "Registry Related Party"), to:

    a. directly or indirectly show any preference or provide any special consideration to any registrar with respect to operational access to registry systems and related registry services, unless comparable opportunities to qualify for such preferences or considerations are made available to all registrars on substantially similar terms and subject to substantially similar conditions;

    b. register domain names in its own right, except for names registered through an ICANN accredited registrar; provided, however, that Registry Operator may (a) reserve names from registration pursuant to Section 2.6 of the Agreement and (b) may withhold from registration or allocate to Registry Operator up to one hundred (100) names pursuant to Section 3.2 of Specification 5;

    c. register names in the TLD or sub-domains of the TLD based upon proprietary access to information about searches or resolution requests by consumers for domain names not yet registered (commonly known as, "front-running"); or

    d. allow any Affiliated registrar to disclose Personal Data about registrants to Registry Operator or any Registry Related Party, except as reasonably necessary for the management and operations of the TLD, unless all unrelated third parties (including other registry operators) are given equivalent access to such user data on substantially similar terms and subject to substantially similar conditions.

2. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will, or will cause such Registry Related Party to, ensure that such services are offered through a legal entity separate from Registry Operator, and maintain separate books of accounts with respect to its registrar or registrar-reseller operations.

3. If Registry Operator or a Registry Related Party also operates as a provider of registrar or registrar-reseller services, Registry Operator will conduct internal reviews at least once per calendar year to ensure compliance with this Code of Conduct. Within twenty (20) calendar days following the end of each calendar year, Registry Operator will provide the results of the internal review, along with a certification executed by an executive officer of Registry Operator certifying as to

Registry Operator's compliance with this Code of Conduct, via email to an address to be provided by ICANN. (ICANN may specify in the future the form and contents of such reports or that the reports be delivered by other reasonable means.) Registry Operator agrees that ICANN may publicly post such results and certification; provided, however, ICANN shall not disclose Confidential Information contained in such results except in accordance with Section 7.15 of the Agreement.

4.   Nothing set forth herein shall: (i) limit ICANN from conducting investigations of claims of Registry Operator's non-compliance with this Code of Conduct; or (ii) provide grounds for Registry Operator to refuse to cooperate with ICANN investigations of claims of Registry Operator's non-compliance with this Code of Conduct.

5.   Nothing set forth herein shall limit the ability of Registry Operator or any Registry Related Party, to enter into arms-length transactions in the ordinary course of business with a registrar or reseller with respect to products and services unrelated in all respects to the TLD.

6.   Registry Operator may request an exemption to this Code of Conduct, and such exemption may be granted by ICANN in ICANN's reasonable discretion, if Registry Operator demonstrates to ICANN's reasonable satisfaction that (i) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator for the exclusive use of Registry Operator or its Affiliates, (ii) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator, and (iii) application of this Code of Conduct to the TLD is not necessary to protect the public interest.

SPECIFICATION 10

REGISTRY PERFORMANCE SPECIFICATIONS

1. **Definitions**

    1.1. **DNS**. Refers to the Domain Name System as specified in RFCs 1034, 1035, and related RFCs.

    1.2. **DNSSEC proper resolution**. There is a valid DNSSEC chain of trust from the root trust anchor to a particular domain name, e.g., a TLD, a domain name registered under a TLD, etc.

    1.3. **EPP**. Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.

    1.4. **IP address**. Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.

    1.5. **Probes**. Network hosts used to perform (DNS, EPP, etc.) tests (see below) that are located at various global locations.

    1.6. **RDDS**. Registration Data Directory Services refers to the collective of WHOIS and Web-based WHOIS services as defined in Specification 4 of this Agreement.

    1.7. **RTT**. Round-Trip Time or RTT refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.

    1.8. **SLR**. Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2. **Service Level Agreement Matrix**

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime (≈ 99%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	≤ 500 ms, for at least 95% of the queries
	DNS update time	≤ 60 min, for at least 95% of the probes
RDDS	RDDS availability	≤ 864 min of downtime (≈ 98%)

	RDDS query RTT	≤ 2000 ms, for at least 95% of the queries
	RDDS update time	≤ 60 min, for at least 95% of the probes
EPP	EPP service availability	≤ 864 min of downtime (≈ 98%)
	EPP session-command RTT	≤ 4000 ms, for at least 90% of the commands
	EPP query-command RTT	≤ 2000 ms, for at least 90% of the commands
	EPP transform-command RTT	≤ 4000 ms, for at least 90% of the commands

Registry Operator is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

3.   **DNS**

3.1.   **DNS service availability**. Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g., a TLD), to answer DNS queries from DNS probes. For the service to be considered available at a particular moment, at least, two of the delegated name servers registered in the DNS must have successful results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" to which the name server resolves. If 51% or more of the DNS testing probes see the service as unavailable during a given time, the DNS service will be considered unavailable.

3.2.   **DNS name server availability**. Refers to the ability of a public-DNS registered "**IP address**" of a particular name server listed as authoritative for a domain name, to answer DNS queries from an Internet user. All the public DNS-registered "**IP address**" of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined/unanswered results from "**DNS tests**" to a name server "**IP address**" during a given time, the name server "**IP address**" will be considered unavailable.

3.3.   **UDP DNS resolution RTT**. Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.4.   **TCP DNS resolution RTT**. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.5.   **DNS resolution RTT**. Refers to either "**UDP DNS resolution RTT**" or "**TCP DNS resolution RTT**".

3.6. **DNS update time**. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, until the name servers of the parent domain name answer "**DNS queries**" with data consistent with the change made. This only applies for changes to DNS information.

3.7. **DNS test**. Means one non-recursive DNS query sent to a particular "**IP address**" (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. A query with a "**DNS resolution RTT**" 5 times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the "**DNS resolution RTT**" or, undefined/unanswered.

3.8. **Measuring DNS parameters**. Every minute, every DNS probe will make an UDP or TCP "**DNS test**" to each of the public-DNS registered "**IP addresses**" of the name servers of the domain name being monitored. If a "**DNS test**" result is undefined/unanswered, the tested IP will be considered unavailable from that probe until it is time to make a new test.

3.9. **Collating the results from DNS probes**. The minimum number of active testing probes to consider a measurement valid is 20 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

3.10. **Distribution of UDP and TCP queries**. DNS probes will send UDP or TCP "**DNS test**" approximating the distribution of these queries.

3.11. **Placement of DNS probes**. Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

4. **RDDS**

4.1. **RDDS availability**. Refers to the ability of all the RDDS services for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable.

4.2.   **WHOIS query RTT**. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

4.3.   **Web-based-WHOIS query RTT**. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

4.4.   **RDDS query RTT**. Refers to the collective of "**WHOIS query RTT**" and "**Web-based- WHOIS query RTT**".

4.5.   **RDDS update time**. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.

4.6.   **RDDS test**. Means one query sent to a particular "**IP address**" of one of the servers of one of the RDDS services. Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDDS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.

4.7.   **Measuring RDDS parameters**. Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered "**IP addresses**" of the servers for each RDDS service of the TLD being monitored and make an "**RDDS test**" to each one. If an "**RDDS test**" result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.

4.8.   **Collating the results from RDDS probes**. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

4.9.   **Placement of RDDS probes**. Probes for measuring RDDS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

5.   **EPP**

5.1.   **EPP service availability**. Refers to the ability of the TLD EPP servers as a group, to respond to commands from the Registry accredited Registrars, who already have credentials to the servers. The response shall include appropriate data from the Registry System. An EPP command with "**EPP command RTT**" 5 times higher than the corresponding SLR will be considered as unanswered. If 51% or more of the EPP testing probes see the EPP service as unavailable during a given time, the EPP service will be considered unavailable.

5.2.   **EPP session-command RTT**. Refers to the **RTT** of the sequence of packets that includes the sending of a session command plus the reception of the EPP response for only one EPP session command. For the login command it will include packets needed for starting the TCP session. For the logout command it will include packets needed for closing the TCP session. EPP session commands are those described in section 2.9.1 of EPP RFC 5730. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.

5.3.   **EPP query-command RTT**. Refers to the **RTT** of the sequence of packets that includes the sending of a query command plus the reception of the EPP response for only one EPP query command. It does not include packets needed for the start or close of either the EPP or the TCP session. EPP query commands are those described in section 2.9.2 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

5.4.   **EPP transform-command RTT**. Refers to the **RTT** of the sequence of packets that includes the sending of a transform command plus the reception of the EPP response for only one EPP transform command. It does not include packets needed for the start or close of either the EPP or the TCP session. EPP transform commands are those described in section 2.9.3 of EPP RFC 5730. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.

5.5.   **EPP command RTT**. Refers to "**EPP session-command RTT**", "**EPP query-command RTT**" or "**EPP transform-command RTT**".

5.6.   **EPP test**. Means one EPP command sent to a particular "**IP address**" for one of the EPP servers. Query and transform commands, with the exception of "create", shall be about existing objects in the Registry System. The response shall include appropriate data from the Registry System. The possible results to an EPP test are: a number in milliseconds corresponding to the "**EPP command RTT**" or undefined/unanswered.

5.7.   **Measuring EPP parameters**. Every 5 minutes, EPP probes will select one "**IP address**" of the EPP servers of the TLD being monitored and make an

"**EPP test**"; every time they should alternate between the 3 different types of commands and between the commands inside each category. If an "**EPP test**" result is undefined/unanswered, the EPP service will be considered as unavailable from that probe until it is time to make a new test.

5.8.   **Collating the results from EPP probes**. The minimum number of active testing probes to consider a measurement valid is 5 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

5.9.   **Placement of EPP probes**. Probes for measuring EPP parameters shall be placed inside or close to Registrars points of access to the Internet across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

6.   **Emergency Thresholds**

The following matrix presents the emergency thresholds that, if reached by any of the services mentioned above for a TLD, would cause the emergency transition of the Registry for the TLD as specified in Section 2.13 of this Agreement.

Critical Function	Emergency Threshold
DNS Service (all servers)	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP	24-hour total downtime / week
RDDS (WHOIS/Web-based WHOIS)	24-hour total downtime / week
Data Escrow	Breach of the Registry Agreement as described in Specification 2, Part B, Section 6.

7.   **Emergency Escalation**

Escalation is strictly for purposes of notifying and investigating possible or potential issues in relation to monitored services. The initiation of any escalation and the subsequent cooperative investigations do not in themselves imply that a monitored service has failed its performance requirements.

Escalations shall be carried out between ICANN and Registry Operators, Registrars and Registry Operator, and Registrars and ICANN. Registry Operators and ICANN must provide said emergency operations departments. Current contacts must be maintained between ICANN and Registry Operators and published to Registrars, where relevant to their role in

escalations, prior to any processing of an Emergency Escalation by all related parties, and kept current at all times.

7.1. **Emergency Escalation initiated by ICANN**

Upon reaching 10% of the Emergency thresholds as described in Section 6 of this Specification, ICANN's emergency operations will initiate an Emergency Escalation with the relevant Registry Operator. An Emergency Escalation consists of the following minimum elements: electronic (i.e., email or SMS) and/or voice contact notification to the Registry Operator's emergency operations department with detailed information concerning the issue being escalated, including evidence of monitoring failures, cooperative trouble-shooting of the monitoring failure between ICANN staff and the Registry Operator, and the commitment to begin the process of rectifying issues with either the monitoring service or the service being monitoring.

7.2. **Emergency Escalation initiated by Registrars**

Registry Operator will maintain an emergency operations department prepared to handle emergency requests from registrars. In the event that a registrar is unable to conduct EPP transactions with the registry for the TLD because of a fault with the Registry Service and is unable to either contact (through ICANN mandated methods of communication) the Registry Operator, or the Registry Operator is unable or unwilling to address the fault, the registrar may initiate an emergency escalation to the emergency operations department of ICANN. ICANN then may initiate an emergency escalation with the Registry Operator as explained above.

7.3. **Notifications of Outages and Maintenance**

In the event that a Registry Operator plans maintenance, it will provide notice to the ICANN emergency operations department, at least, twenty-four (24) hours ahead of that maintenance. ICANN's emergency operations department will note planned maintenance times, and suspend Emergency Escalation services for the monitored services during the expected maintenance outage period.

If Registry Operator declares an outage, as per its contractual obligations with ICANN, on services under a service level agreement and performance requirements, it will notify the ICANN emergency operations department. During that declared outage, ICANN's emergency operations department will note and suspend emergency escalation services for the monitored services involved.

8. **Covenants of Performance Measurement**

8.1. **No interference**. Registry Operator shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registry Operator shall respond to the measurement tests described in this Specification as it would to any other request from an Internet user (for DNS and RDDS) or registrar (for EPP).

8.2. **ICANN testing registrar**. Registry Operator agrees that ICANN will have a testing registrar used for purposes of measuring the **SLR**s described above. Registry Operator agrees to not provide any differentiated treatment for the testing registrar other than no billing of the transactions. ICANN shall not use the registrar for registering domain names (or other registry objects) for itself or others, except for the purposes of verifying contractual compliance with the conditions described in this Agreement.

SPECIFICATION 11

PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on 27 June 2013 in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. (Intentionally omitted. Registry Operator has not included commitments, statements of intent or business plans provided for in its application to ICANN for the TLD.)

3. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

   a. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

   b. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

   c. Registry Operator will operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies.

   d. Registry Operator of a "Generic String" TLD may not impose eligibility criteria for registering names in the TLD that limit registrations exclusively to a single person or entity and/or that person's or entity's "Affiliates" (as

defined in Section 2.9(c) of the Registry Agreement). "Generic String" means a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others.

4. Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

The above Section 4 of this Specification applies to the following public interest commitments of Registry Operator related to the TLD. Nothing in Section 4 of this Specification shall limit any obligations of Registry Operator under Sections 1, 2 and 3 of this Specification. In the event Section 4 of this Specification conflicts with the requirements of any other provision of the Registry Agreement (including any Section of this Specification), such other provision shall govern.

    a. **Open registration** - Second level registrations in the TLD will be open and available to lawful registrants. The TLD represents a generic or dictionary term, and Registry Operator accordingly will operate it in an inclusive manner. Registry Operator will not limit registrant eligibility based on identity nor restrict availability of second level names to only registrants whose identity is associated only with the most common usage of the term. Registry Operator will not disenfranchise lawful users who are associated with a minority usage of the term.

    b. **Geographic name protection** - Pursuant to Specification 5 of this Registry Agreement, Registry Operator will transmit to registrars the list of geographic names prohibited from second level registration. Registry Operator will periodically review this list to ensure it is identical to that maintained by ICANN. Should Registry Operator seek to release these reserved names, it will consult with ICANN's Governmental Advisory Committee and obtain any permissions necessary from ICANN for such release.

    c. **Rights Protection Mechanisms and Abuse Mitigation** - Registry Operator commits to implementing and performing the following protections for the TLD:

i. In order to help registrars and registrants identify inaccurate data in the Whois database, Registry Operator will audit Whois data for accuracy on a statistically significant basis.

ii. Work with registrars and registrants to remediate inaccurate Whois data to help ensure a more accurate Whois database. Registry Operator reserves the right to cancel a domain name registration on the basis of inaccurate data, if necessary.

iii. Establish and maintain a Domains Protected Marks List (DPML), a trademark protection service that allows rights holders to reserve registration of exact match trademark terms and terms that contain their trademarks across all gTLDs administered by Registry Operator under certain terms and conditions.

iv. At no cost to trademark holders, establish and maintain a Claims Plus service, which is a notice protection mechanism that begins at the end of ICANN's mandated Trademark Claims period.

v. Bind registrants to terms of use that define and prohibit illegal or abusive activity.

vi. Limit the use of proxy and privacy registration services in cases of malfeasance.

vii. Consistent with the terms of this Registry Agreement, reserve the right to exclude from distribution any registrars with a history of non-compliance with the terms of the Registrar Accreditation Agreement.

viii. Registry Operator will be properly resourced to perform these protections.

d. **Anti-Abuse Policy**

i. Registry Operator's Anti-Abuse Policy will be required under the Registry Registrar Agreement and posted on the Registry Operator's web site.

ii. Registry Operator will monitor the TLD for abusive behavior and address it as soon as possible if detected.

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

   A.   to protect the integrity and stability of the registry;

   B.   to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;

   C.   to comply with the terms of this Registry Agreement and the Registry Operator's Anti-Abuse Policy;

   D.   registrant fails to keep Whois information accurate and up-to-date;

   E.   domain name use violates the Registry Operator's acceptable use policies, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark; or

   F.   as needed during resolution of a dispute.

iv.   <u>Abuse Point of Contact</u>. Registry Operator will provide an abuse point of contact (APOC). This contact will be a role-based e-mail address posted on the Registry Operator's web site in the form such as abuse123@registry.tld. This e-mail address will allow multiple staff members to monitor and address abuse reports. Registry Operator will further provide a convenient web form for complaints.

The public interest commitments set forth in this Section 4 of this Specification shall be subject to review by Registry Operator starting in January 2016, and Registry Operator, in its sole discretion and upon written notice to ICANN, may elect at that time to discontinue any of such public interest commitments in the case of a substantial and compelling business need.

ATTACHMENT 5
(Decision – Majority Ruling)

THE INTERNATIONAL CENTRE FOR EXPERTISE OF THE

INTERNATIONAL CHAMBER OF COMMERCE

CASE No. EXP/412/ICANN/29

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR

(FRANCE)

vs/

RUBY PIKE, LLC

(USA)

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.

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

THE EXPERT DETERMINATION

issued by the Expert Panel,
composed of

Mr. Piotr Nowaczyk (Chair)
e-mail:
Contact Information Redacted

Prof. August Reinisch
e-mail:
Contact Information Redacted

Contact Information Redacted

Contact Information
Redacted

Mr. Ike Ehiribe
e-mail:
Contact Information
Redacted

Contact Information Redacted

in Case No.
EXP/412/ICANN/29

PROF. ALAIN PELLET, INDEPENDENT OBJECTOR (FRANCE) v. RUBY PIKE, LLC (USA)

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

Name	Abbreviation
Rules for Expertise of the ICC	"**Rules**"
Appendix III to the ICC Expertise Rules, Schedule of expertise costs for proceedings under the new gTLD dispute resolution procedure	"**Appendix III**"
International Chamber of Commerce	"**ICC**"
ICC Practice Note on the Administration of Cases	"**ICC Practice Note**"
Attachment to Module 3 - New gTLD Dispute Resolution Procedure	"**Procedure**"
Module 3 of the gTLD Applicant Guidebook	"**Guidebook**"
The Independent Objector - prof. Alain Pellet (France)	"**IO**"
The Applicant - Ruby Pike, LLC (USA)	"**Applicant**"
The Applicant's parent company Donuts, Inc.	"**Donuts**"
ICC International Centre for Expertise	"**Centre**"
Domain name search tool	"**WHOIS**"
Prof. August Reinisch (co-expert), Mr. Ike Ehiribe (co-expert) and Mr. Piotr Nowaczyk (chair) appointed by the Centre to render Expert Determination	"**Expert Panel**"
Governmental Advisory Committee	"**GAC**"

- 4 -

Identification of the Parties, their Representatives and related entities

Objector

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

Objector's Representative(s)

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

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

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

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

Applicant

Name	Ruby Pike, LLC
Contact person	Mr. Daniel Schindler, Mr. John Nevett
Address	Contact Information Redacted
City, Country	
Telephone	
Email	

Applicant's Representative(s)

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

Disputed gTLD

gTLD Objector objects to [.example]

Name	.Hospital (Application ID: 1-1505-15195)

I. PARTIES

1. The objector in this case is the Independent Objector (hereafter referred to as the "**IO**"), Prof. Alain Pellet, appointed by ICANN to serve for the entire new gTLD program and object to highly objectionable gTLD applications on Limited Public Interest and Community grounds as it is stated in paragraph 3.2.5 of the Guidebook.

2. The Applicant (hereafter referred to as the "**Applicant**") is an American company – Ruby Pike, LLC, an affiliate of Donuts, Inc. which has applied for 307 new gTLDs representing a variety of common dictionary names.

II. PROCEDURAL HISTORY

3. On 12 March 2013, the IO filed via email a Limited Public Interest Objection against the Application of Ruby Pike LLC, for the gTLD string .Hospital (Application ID: 1-1505-15195). Copies of the Objection were transmitted via email to the Applicant and to ICANN on 13 March 2013.

4. On 29 March 2013, the Dispute Resolution Service Provider, namely the International Centre for Expertise (hereafter referred to as the "**Centre**") of the International Chamber of Commerce (hereinafter referred to as the "**ICC**") informed the IO that it had conducted an administrative review of the Objection (Article 9 of the Procedure) and that the Objection was in compliance with Articles 5 - 8 of the Procedure and with the Rules.

5.   On 15 April 2013, the Centre further informed the Parties that ICANN had published its Dispute Announcement pursuant to Article 10(a) of the Procedure on 12 April 2013. It invited the Applicant to file a Response within 30 days of the transmission of this invitation (Article 11 (b) of the Procedure).

6.   On 15 May 2013, the Applicant filed via email its Response to the Objection with Annexes. Copies were transmitted to the IO and its representatives, as well as to ICANN.

7.   On 28 May 2013, the Centre informed the Parties that the Response was in compliance with Article 11 of the Procedure and with the Rules and confirmed receipt of the Applicant's payment of the Filing Fee in the amount of EUR 5,000.

8.   On 19 June 2013, the Centre informed the Parties that the Chairman of the Standing Committee of the Centre appointed Mr. Piotr Nowaczyk as the Chairman of the Expert Panel and Prof. August Reinisch, and Mr. Ike Ehiribe as Co-Experts on the Expert Panel. The Centre also invited both Parties to make the required advance payment of costs for the Expert Panel to be fully constituted.

9.   On 1 August 2013, the Centre confirmed receipt of the Parties' required advance payment and transferred the case file to the Expert Panel after confirmation of the full constitution of the Expert Panel.

10.   By an email of 2 August 2013, the IO requested to file an additional written statement in order to address new issues that were raised in the Applicant's Response. The Expert Panel granted this request. In Procedural Order No. 1 dated 5 August 2013 it set a deadline of 12 August 2013 for the IO's additional written statement. In its Procedural Order No. 2 dated 9 August 2013 the Expert Panel clarified, at the request of the Applicant, that the scope of the additional written statement shall be limited to: (1) the allegation of bias raised by the Applicant; and (2) the interpretation of the new gTLD Dispute Resolution Procedure.

11.   The IO accordingly filed the additional written statement via email on 12 August 2013. Electronic copies were transmitted to the Applicant and its representatives, as well as to ICANN.

12.   In Procedural Order No. 3 dated 13 August 2013, the Expert Panel set a deadline of 20 August 2013 for the Applicant's response to the IO's additional written statement and limited the scope of the response to the matters raised in the IO's additional written statements. The Applicant's response was submitted accordingly on 20 August 2013. Electronic copies were transmitted to the IO and its representatives, as well as to ICANN.

13.   In Procedural Order No. 4 dated 28 August 2013, the Expert Panel acknowledged that the Objection was not dismissed in the course of the Quick Look Procedure for the reasons that would be presented in an Expert Determination.

14.   Pursuant to Article 6(a) of the Procedure, all communications by the Parties, the Expert Panel and the Centre were submitted electronically.

15.   There was no hearing in this case, as the Expert Panel decided it was not necessary, as well as, it was not requested by the parties.

16.   The draft Expert Determination was transmitted for scrutiny to the Centre within the 45 day time limit in accordance with Article 21 (a) and (b) of the Procedure.

III.   APPLICABLE RULES AND THE LANGUAGE OF THE DISPUTE RESOLUTION PROCEDURE.

17.   All proceedings before the Expert Panel shall be governed by the following rules:

- Rules for Expertise of the ICC (hereafter referred to as the "**Rules**"),

- The ICC Practice Note on the Administration of the Cases (hereafter referred to as the "**ICC Practice Note**"),

- Attachment to Module 3 of the gTLD Applicant Guidebook, New gTLD Dispute Resolution Procedure of the gTLD Applicant Guidebook (hereafter referred to as the "**Procedure**"),

- ICANN gTLD Applicant Guidebook (hereafter referred to as the "**Guidebook**").

18. The language of all submissions and proceedings is English (Art. 5(a) of the Procedure).

IV. PARTIES' CONTENTIONS

A. The Independent Objector

19. The IO confirms that he is not affiliated with any of the gTLD applicants and remains impartial and independent as required under the Guidebook. Responding to the Applicant's allegation of bias, the IO stated that he has not favoured any particular interests, including medical interests and that he has not targeted the Applicant's Application since he has filed objections against gTLD applications for strings entirely unrelated to health and the healthcare sector, including .Amazon, .Charity, .Indians and .Patagonia.

20. The IO asserts that he acts pursuant to paragraph 3.2.5 of the Guidebook, providing him with the standing to file the Objection, since there was more than one comment made in opposition to the Application in the public domain. Later, the IO also asserts that the above-mentioned procedural restriction concerning his standing did not allow him to file objections to other sensitive applications.

21. The IO asserts that the Limited Public Interest Objection is applicable in this case since the applied-for gTLD string is contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law based exclusively on the fourth ground, which stipulates as follows:

"A determination that an applied-for gTLD string would be contrary to specific principles of international law as reflected in relevant international instruments of law." (paragraph 3.5.3 of the Guidebook)

22. The IO states that while the Objection is against the applied-for gTLD string, however, in addition, it should be considered in the context of the stated intended purpose as it may be derived from the description of the Applicant's position provided especially in the section titled "Mission/Purpose" (Section 18) in the Application form. Therefore, the IO does not find the applied-for string to be objectionable *per se*, but that the applied-for string and its intended operation may be objectionable from the perspective of specific principles of international law for morality and public order. The IO argues further that the Applicant's Application as presented does not guarantee the use of the applied-for string in full respect of these general principles of international law for morality and public order.

23. The IO recognizes the importance of freedom of expression as, also, a general principle of international law relating to morality and public order. At the same time, according to the IO, freedom of expression is not free of any limits but "*carries with it special duties and responsibilities*" (Guidebook, paragraph 3.5.3, at p. 3-22). The concept of raising Limited Public Interest Objections implies that these limits may lead to the rejection of certain applied-for strings.

24. The IO provides a comprehensive deliberation regarding the validity of his Objection. The Applicant has itself recognized that the gTLD is "*attractive to registrants with a connection to hospitals and medical treatment centers around the world.*". In the IO's view, hospitals are inextricably connected to health, which is commonly deemed to be a fundamental human right under international law instruments. In support, the IO refers to, among others, the following instruments of international law :

- the proclamation of the Universal Declaration of Human Rights the General Assembly of the United Nations which has declared "health" to be part of this listing of Human Rights (*Article 25, (1) Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and* **medical care** *and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control.*);

- the International Covenant on Economic, Social and Cultural Rights (*Article 12 (1) The States Parties to the present Covenant recognize* **the right of everyone to the enjoyment of the highest attainable standard of physical and mental health**);

- International Convention on the Elimination of All Forms of Racial Discrimination (*Article 5 (e) Economic, social and cultural rights, in particular: (iv)* **The right to public health, medical care**, *social security and social services*);

- Convention on the Elimination of All Forms of Discrimination against Women *(Article 11 (1) States Parties shall take all appropriate measures to eliminate discrimination against women in the field of employment in order to ensure, on a basis of equality of men and women, the same rights, in particular (f) The* **right to protection of health** *and to safety in working conditions, including the safeguarding of the function of reproduction. And Article 12 1. States Parties shall take all appropriate measures to eliminate discrimination against women in the field of health care in order to ensure, on a basis of equality of men and women,* **access to health care services,** *including those related to family planning. 2. Notwithstanding the provisions of paragraph I of this article, States Parties shall ensure to women appropriate services in connection with pregnancy, confinement and the post-natal period, granting free services where necessary, as well as adequate nutrition during pregnancy and lactation*);

- Convention on the Rights of the Child (*Article 24 - 1. States Parties recognize* **the right of the child to the enjoyment of the highest attainable standard of health** *and to facilities for the treatment of illness and rehabilitation of health. States Parties shall strive to ensure that no child is deprived of his or her right of access to such health care services. 2. States Parties shall pursue full implementation of this right and, in particular, shall take appropriate measures: (e) To ensure that all segments of society,* **in particular parents and children, are informed, have access to education and are supported in the use of basic knowledge of child health** *and nutrition, the advantages of breastfeeding, hygiene and environmental sanitation and the prevention of accidents*);

- Convention on the Rights of Persons with Disabilities (*Article 25 - Persons with disabilities have the right to* **the highest attainable standard of health without discrimination on the basis of disability.** *They are to receive the same range, quality and standard of free or affordable health services as provided other persons, receive those health services needed because of their disabilities, and not to be discriminated against in the provision of health insurance*),

- WHO Constitution dated 22 July 1945 – "The enjoyment of the highest *attainable standard of* **health is one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social condition.** *The health of all peoples is fundamental to the attainment of peace and security and is dependent upon the fullest co-operation of individuals and States. (...) The extension to all peoples of the benefits of medical, psychological and related knowledge is essential to the* **fullest attainment of health**".[1]

25. The IO asserts that the International Covenant on Economic, Social and Cultural Rights imposes on the parties the obligation to assure the right to health. By referring to the comments of the United Nations Committee on Economics, Social and Cultural Rights, the IO connects the above-mentioned obligation with the duty to guarantee accessibility and quality of health care facilities. Therefore, as the IO later asserts, states providing misleading health-related information violate their obligations under the Covenant. In this regard the IO refers to an European Court of Human Rights decision in *Guerra and others v. Italy*, [1998] ECHR 7, 26 EHRR 357, where the failure of a state to provide essential information relating to environmental pollution that would have enabled the applicants to assess the risk they and their families would be exposed to in a particular town was found to be tantamount to a violation of the applicant's right to respect for private and family life in breach of Article 8 of the European Convention of Human Rights.

26. The IO also states that not only public authorities, but also the private sector has responsibilities as regards the protection of human rights. In the IO's opinion the Applicant has not given due consideration to the fundamental rights and related obligations that are at stake and has not considered how to include safeguard mechanisms that at all times would rather strengthen instead of hindering these obligations and fundamental rights.

27. The IO is of the view that the Applicant should demonstrate how, given the public interest at stake, the policies and decision-making of the Applicant will be properly connected to the public authorities, national as well as international, that are under a legal obligation to respect, protect and fulfill the right to health.

28. Moreover, the IO points out that the Applicant's parent company Donuts has applied for over 300 gTLDs and that the texts of those applications all seem to be entirely identical although the applied-for strings have a completely different character.

29. The IO argues that the fact that the additional four protection mechanisms employed by the Applicant for .Hospital are present in many of Donuts' applications that are completely unrelated to health confirms the Applicant's lack of awareness of the specifics of health-related gTLDs like the present one.

30. Since the Applicant did not provide any insight on the extent or content of the social consultations that were allegedly conducted, the IO maintains his Objection to the instant Application as long as the Applicant does not - after consultation and coordination with all stakeholders of the health community, including states and competent international organizations – provide solutions for the serious concerns raised by the IO and other entities in the past.

31. In his additional written statements, the IO refers to the Safeguard Advice issued by ICANN's Governmental Advisory Committee (GAC) on 11 April 2013 which states that extensive additional safeguards should be put in place for a whole range of gTLDs including .Hospital. According to the IO, this confirms the concerns expressed in the Objection and the sensitivity

---

[1] The emphasis is added by the Expert Panel in order to underline the relation to health and healthcare.

of a new .Hospital gTLD and demonstrates that those concerns are not to be considered as abusive, nor as harassment as alleged by the Applicant.

32.   The IO requests the Expert Panel to hold that the Objection is valid. Therefore, the Expert Panel should uphold the present Objection against the .Hospital Application.

33.   In the alternative, the IO requests the Expert Panel to hold that the Objection is valid as long as the Applicant does not provide solutions for the serious objections raised above. Accordingly, the Expert Panel should conditionally uphold the present Objection against the .Hospital Application (ID: 1-1505-15195).

34.   In addition, the IO requests that its advance payments of costs shall be refunded in accordance with Article 14 (e) of the Procedure.

B.   The Applicant

35.   The Applicant is an American limited liability company owned by Donuts, through which the Applicant and other direct and indirect subsidiaries, have applied for 307 new gTLDs representing a variety of common dictionary terms. The Applicant introduces itself as a well-prepared, amply resourced and highly qualified organization committed to offering consumers new and varied generic domain name alternatives through safe, stable and secure registry operations.

36.   The Applicant declares that it seeks to help redefine the domain name space in the Internet by offering domains that would serve a more specific segment of the Internet user population. The Applicant repeatedly identifies itself with goals explicitly articulated by ICANN in specific connection with its new gTLD program such as: augmenting consumer choice, bolstering competition and expanding avenues of expression on the Internet.

37.   In its response, the Applicant challenges the IO's independence, relying upon the following arguments:

-   The IO has filed relatively few objections overall, and Donuts' applications represent a significant proportion of them,

-   The IO has brought objections only against applications for health-related gTLDs and has not brought such objections against other controversial gTLDs,

-   The IO has a background in health-related matters and particular healthcare and policy interests since he has worked in co-operation with the World Health Organization (WHO),

-   The IO's legal assistant has alleged relationship with a WHO consultant.

38.   In the Applicant's view, the IO clearly has some bias that favours healthcare and hospital interests and opposes those who would provide a forum for such topics on the Internet.

39.   The Applicant seeks the dismissal of this Objection following the Quick Look Procedure since it is, in the Applicant's opinion, manifestly unfounded. As the Applicant asserts, the ICANN's standards focus on the string itself not on the Applicant whereas the IO simply criticizes its activity, putting the instant Application aside. Such attacks in the Applicant's view may amount to "an abuse of the right to object."

40.   The Applicant states that the Objection is based on nothing more than speculation regarding matters beyond the applied-for string or its intended use as stated in the Application. Then, it is acknowledged that the applied-for string is nothing more than the generic term "hospital" which can be used in a variety of perfectly legitimate ways, none of which are "contrary to morality and public order." The Applicant also provides examples of the use of the word "hospital" as a second level domain in a context that is unrelated to the medical sector.

41. The Applicant states that the Objection is unfounded because it does not fall within the scope of the ground on which the IO relied (paragraph 3.5.3 of the Guidebook). Moreover, the Applicant argues that the fourth ground cannot be interpreted so broadly, since it would be inconsistent with the idea of the whole provision. The Applicant refers to the commonly known rule of interpretation - *ejusdem generis* ("of the same kinds, class, or nature") - and concludes that the norms of international law quoted in the Objection do not belong to the same category of topics as genocide, torture, slavery, violence against women, racism, and child pornography/sexual abuse, which are included in the first three grounds.

42. In the Applicant's view, the IO offers no evidence to meet the Objector's significant burden of proof since the Objection relies upon, among others, such innocuous and amorphous factors:

   - Whether Donuts affiliates have applied for three, three hundred or three thousand TLDs does not prove that the TLD applied for here will breach any international law restrictions;

   - Whether the instant Application resembles or differs from the over 300 others submitted by related entities neither proves that the string does, nor demonstrates that Applicant intends to, violate widely accepted international law norms against violent, discriminatory, sexually abusive or similarly egregious behaviour.

43. Furthermore, the Applicant claims that the IO arguably infringes upon the Applicant's and the public's rights to freedom of expression. As the Applicant supports an open gTLD, and believes in permitting the public to exercise freedom of expression unless such use violates the law, it disagrees with the policy position taken by the IO.

44. The Applicant also remarks that it is the only applicant for the .Hospital applied-for string. Therefore, if the IO succeeds in his Objection, the gTLD will not be available to any members of the public.

45. The Applicant acknowledges its intention to operate open and unrestricted gTLDs for the benefit of all law-abiding users. The Applicant calls the Expert Panel to bear in mind, however, that — as is the case in all forms of progress — there may be some level of cost. Further, the net benefit to the worldwide community should be recognized instead of closing off great sections of opportunity due to perceived possible, though unlikely, harm.

46. As the Applicant asserts, it should be noted that the term "hospital" is usually used in numerous second-level domain names. The Applicant has found over 26,000 uses in second-level domain names of the same term that the IO here claims will run afoul of international precepts of morality and public order.

47. Moreover, the Applicant finds the opinion issued by ICANN's Government Advisory Committee ("**GAC**") and recalled by the IO even supportive for its Application since the Applicant implements most of additional safeguards sought by the Committee. Then, the Applicant states that there were no restrictions yet accepted by the ICANN's Board as to .Hospital. In the Applicant's view, the present comments of GAC regarding potentially "sensitive strings" constitute the second form of GAC Advise as provided by Guidebook: "(ii) *The GAC advises ICANN that there are concerns about a particular application "dot-example." The ICANN Board is expected to enter into dialogue with the GAC to understand the scope of concerns. The ICANN Board is also expected to provide a rationale for its decision*". Therefore, such advice has no relevance to the instant Objection because ICANN has no obligation to adopt all or any of the GAC recommendations regarding the subject string.

48. Therefore, the Applicant requests the Expert Panel to deny the Objection.

V.   DISCUSSION AND REASONING

49.   The Expert Panel is required to make the Expert Determination in accordance with the standards provided in Article 20 of the Procedure which states as follows:

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

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

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

50.   Thus, the Expert Panel is bound also by the standards defined by ICANN. Paragraph 3.5.3 of the Guidebook, which is applicable to the case under consideration, and which states that "*An expert panel hearing a Limited Public Interest objection will consider whether the applied-for gTLD string is contrary to general principles of international law for morality and public order.*" The same paragraph provides a non-exhaustive list of international law instruments containing such principles which includes among others:

-    The Universal Declaration of Human Rights (UDHR) (1948),

-    The International Covenant on Economic, Social, and Cultural Rights (1966), etc.

51.   As is later stated: "*Under these principles, everyone has the right to freedom of expression, but the exercise of this right carries with it special duties and responsibilities. Accordingly, certain limited restrictions may apply.*"

52.   Most essentially, paragraph 3.5.3 also specifies grounds upon which an applied-for gTLD string may be considered contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law such as:

-    Incitement to or promotion of violent lawless action;

-    Incitement to or promotion of discrimination based upon race, color, gender, ethnicity, religion or national origin, or other similar types of discrimination that violate generally accepted legal norms recognized under principles of international law;

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

-    A determination that an applied-for gTLD string would be contrary to specific principles of international law as reflected in relevant international instruments of law.

53.   Paragraph 3.5.3 also instructs the Expert Panel to conduct its analysis on the basis of the applied-for gTLD string itself. The Expert Panel may, if needed, use as additional context the intended purpose of the gTLD as stated by the Applicant in its Application.

54.   The Expert Panel has considered those standards listed above, the relevant international law instruments and relevant case law cited by the IO and has reasoned as follows.

A.   The IO's alleged bias

55.   Paragraph 3.2.5 of the Guidebook requires the IO to be independent of and unaffiliated with any of the gTLD applicants; however, it does not state any procedural consequences within the objection procedure for breaching these obligations.

56.   Having considered the procedural requirements that the IO is obligated to fulfill in order to file a valid objection, the Expert Panel does not accept the Applicant's assertion that the IO's objections are unduly directed at the Applicant as alleged. The Expert Panel is satisfied that

the IO is acting in the best interest of the public who use the Internet and has filed this Objection in the public interest.

57.   The Applicant's allegations concerning the IO's bias favouring healthcare or medical interests are also unfounded for lack of any verifiable evidence to substantiate such allegations. The Expert Panel accepts, contrary to the Applicant's assertion and as contended by the IO that the IO only acted for the French Republic as Counsel in an advisory proceeding concerning a request by the World Health Organization which came before the International Court of Justice. Just for the sake of completeness, the Expert Panel equally finds no merit in the alleged relationship said to be existing between the IO's legal assistant and a consultant of the World Health Organization which in any event the Applicant failed to substantiate by furnishing credible supporting evidence. Thus, the Expert Panel finds that the Applicant's challenge to the IO's independence and impartiality is manifestly unfounded.

B.   The IO's standing

58.   Pursuant to paragraph 3.2.5 of the Guidebook, the IO may file Limited Public Interest Objections against "highly objectionable" gTLD applications to which no objection has been filed. Moreover, the IO shall not object to an application unless at least one comment in opposition to the Application is made in the public sphere.

59.   The Expert Panel finds that the foregoing conditions were satisfied by the IO in these proceedings. Indeed, there was no other Limited Public Interest Objection against .Hospital. Since the importance of hospitals' role for the safety and health of a society cannot be overrated, the instant Application can be deemed to be highly objectionable. Furthermore, the IO states that there were several (10) comments that were made at https://gtldcomment.icann.org/comments-feedback/applicationcomment/viewcomments in opposition to the Application in the public domain.

60.   In any event the Expert Panel has taken into account various other comments in the public domain which were brought to its attention by the IO. Specifically, the Expert Panel refers to the letter dated 11 April 2012 from the World Health Organization seeking a postponement of the assignment of .health related top level domains, and expressing concerns on the likelihood of the illegal promotion and sale of medicines including spurious/falsely–labeled/counterfeit and unapproved medicines through such .health related domains. The second is the Safeguard Advice issued by ICANN's Governmental Advisory Committee (GAC) on 11 April 2013 wherein the applied-for gTLD .Hospital is listed as one of the applied-for strings that requires extensive further safeguards such as: (i) increased WHOIS verification and checks; (ii) expanded terms of use by registry operators to mitigate abusive activity; (iii) increased security checks by Registry operators, constant record keeping by registry operators to identify frequent inaccurate WHOIS records and security threats; (iv) provision of mechanisms for the handling of complaints by registry operators arising from the provision of inaccurate WHOIS information or the facilitation of infringement activity contrary to applicable law; and (v) the identification of real and immediate consequences for providing inaccurate WHOIS information and engaging in infringement or unlawful activity.

61.   The Expert Panel considers that the recent Resolution adopted by the World Health Assembly on 27 May 2013 on eHealth standardization and interoperability also confirms the IO's concerns relating to the applied-for gTLD, .Hospital. The World Health Assembly is recorded to have commented on health related global top-level domain names as follows: "(...) health-related global top-level domain names in all languages, including ".health", should be operated in a way that protects public health, including by preventing the further development of illicit markets of medicines, medical devices and unauthorized health products and services (...)." Therefore, the Expert Panel rejects the Applicant's allegations questioning the IO's standing.

C. The scope of the Limited Public Interests Objection

62. The scope of the Limited Public Interest Objection is expressly limited to the four grounds enumerated in paragraph 3.5.3 of the Guidebook. The fourth and relevant ground to these proceedings being ("contrary to generally accepted legal norms relating to morality and public order (...) recognized under principles of international law").

63. Although the list of grounds in paragraph 3.5.3 includes "or" instead of "and" so as the IO has asserted, there is no conjunction, the wording of this paragraph clearly indicates that this catalogue has an exhaustive character.

64. The fourth ground is an open clause that can be a subject of exemplification. The Expert Panel shares the Applicant's view that according to the *ejusdem generis* doctrine the fourth ground should be interpreted in order to establish a relatively homogenous class of grounds. In this case, it is a class of various violations of human rights.

65. However, the Expert Panel cannot agree with the conclusion that violation of the right to health under the fourth ground is less serious than for example "incitement to or promotion of violent lawless action" which is a violation of right to life and basic freedom.

66. In the Expert Panel's view, human rights such as right to life, freedom from slavery or personal immunity that are covered by the three first grounds are equally as important as the right to health. Thus, an objection against an application that is contrary to the right to health, a fundamental human right as is incorporated in international law instruments falls within the scope of the Limited Public Interests Objection.

D. The Quick Look Procedure

67. As was stated in Procedural Order No. 4 dated 28 August 2013, the Expert Panel did not dismiss the Objection under the Quick Look Procedure, which is aimed at eliminating frivolous and/or abusive objections.

68. Firstly, a Limited Public Interest Objection would be manifestly unfounded if it did not fall within one of the categories that have been defined as grounds for such an objection. As has been demonstrated above, the Objection falls within the fourth ground, which is stated in paragraph 3.5.3 of the Guidebook.

69. Secondly, in accordance with paragraph 3.2.2.3 a Limited Public Interest Objection should be dismissed when it abuses the right to object. The Expert Panel rejects the Applicant's argumentation that the IO attacks it rather than the applied-for string. As is clarified in the next section, the objection may provide additional context for the applied-for string. All the information about the Applicant provided in the Objection is admissible and is not found by the Expert Panel to be abusive, if it is connected with the purpose of operating the present gTLD.

70. Taking into consideration that the Applicant's parent company Donuts, has applied for multiple gTLDs, it is not surprising that a significant portion of the IO's objections were filed against Donuts' applications. Moreover, as was stated before, the procedural requirement for the IO is a veritable safeguard against frivolous objections. Therefore, there are no grounds to justify the Applicant's contention that the Objection is abusive or aimed at harassing the Applicant.

E. The Application should be reviewed in light of its purpose

71. As the Applicant argues, the Guidebook expressly refers to an "applied-for gTLD string"; however, Paragraph 3.5.3 also authorizes the Expert Panel to use as additional context the intended purpose of the gTLD as stated in the Application to conduct its analysis on the basis of the applied-for gTLD string itself. The Applicant clearly states in answer to question 18 of the Application that the Applicant: *"intends to increase competition and consumer choice at the top level (...) In doing so, the TLD will introduce significant consumer choice and competition*

to the Internet namespace – the very purpose of ICANN's new TLD program." Moreover, pursuant to Article 20(b) of the Procedure, the Expert Panel may refer to and base its findings upon the statements and documents submitted and any rules or principles that it determines applicable. Because of the manner that the case has been presented by the parties, the Expert Panel, in deciding on the instant case, considers all the elements: .Hospital and the Applicant's purpose as well as other arguments raised by the IO. Since the procedure is designed to serve the best interest of the public who use the global Internet, the review cannot be limited only to the applied-for string that is just a signboard for the tremendous amount of information. Which information finally is going to be available for users depends on the intended purpose of the Applicant who stands for .Hospital and its acts. Therefore, in the Expert Panel's view, limiting the scope of procedure only to the name of gTLD may render the entire objection procedure pointless.

72. In the Expert Panel's opinion the Applicant's sole purpose for the Application as expressed in the Application documents is simply for commercial purposes. The Application supports the idea of unlimited availability of the instant gTLD for all Internet users. It presents simply a "market approach" whereas morality and public order require a "social approach" as is stated in following sections.

73. It is significant that the Applicant's answer to question *"18(c). What operating rules will you adopt to eliminate or minimize social costs?"* is completely meritless since it concerns only prices for registering second level domains. Such a disregard for social cost of operating .Hospital provides a very clear ind ication of the commercial purpose and mission of the Application.

F.   Burden of proof

74. Article 20 c) of the Procedure requires the IO to prove that the Objection should be sustained in accordance with the applicable standards. In this case the standard, provided by paragraph 3.5.3, is the following: *"an applied-for gTLD string may be considered contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law (...) as reflected in relevant international instruments of law."* Therefore, the IO has to provide the necessary evidence that the Application is indeed contrary to those norms.

75. The Expert Panel finds that there is no binding provision, in either the Guidebook or the Procedure, stating a clear presumption in favour of the Application as the Applicant many times asserts. In the Application, the Applicant refers to archival notes of ICANN that allegedly provide such a presumption, but they no longer exist. Moreover, the Expert Panel is not obligated to follow all ICANN bylaws or its analysis.

G.   The Application is contrary to generally accepted legal norms relating to morality and public order

76. In order to review the case under consideration, the Expert Panel has adopted, on its own initiative, definitions of "morality" and "public order" that are based upon common understanding and respective scientific sources.

77. Morality in the normative sense refers to a code of conduct that applies to all who can understand it and can govern their behaviour by it. Morality should never be overridden, that is, no one should ever violate a moral prohibition or requirement for non-moral considerations. All of those who use "morality" normatively also hold that, under plausible specified conditions, all rational persons would endorse that code (Stanford Encyclopedia of Philosophy, http://plato.stanford.edu/entries/morality-definition/, 09.09.2013). In the present case, the concept of morality is used jointly with the concept of public order.

78. Public order (or *ordre public* in French) has the same meaning as the term "public policy", used especially in Anglo-American legal terminology. Thus, the notion of public order is often used interchangeably with the term "public policy" (Josef Mrazek, Public Order (Ordre Public) and Norms of Ius Cogens in Czech Yearbook of International Law, Public Policy and Ordre Public 2012, p. 79-80). Despite this terminological confusion, public order is commonly understood as the pillar of the legal system and social order. The civil law system recognizes public order as a long-term constant and one upon which rests, not only, the constitutional and legal order. However, in light of the common law approach this term also represents a much broader legislative category which expresses to a certain degree the prevailing political view of social priorities. The Expert Panel adopts the broader notion of public order (public policy) which is close to the category of public interests and goes beyond the interest of individuals (Alexander J. Belohlavek, Public Policy and Public Interest in International Law and EU Law in Czech Yearbook of International Law, Public Policy and Ordre Public 2012, p. 118-119). Such a notion is aimed to ensure the safety and welfare of the society.

79. Morality and public order require all members of society, whether public or private entities, to be extremely cautious on issues of human life and health. It is a duty that should be fulfilled in the field of the development of the Internet as well.

80. The term "Hospital" is a generic term that is commonly associated with healthcare and emergency. This original meaning and health related connotation cannot be replaced or obscured by the commercial use of this name.

81. Misuse of the word "hospital" may cause significant harm to society. The market approach presented by the Applicant greatly increases that risk. The examples of second level domains given by the Applicant that are not related to healthcare but are welcomed to register at ".Hospital" might be a source of mistakes leading to endangering health or life.

82. It is important to bear in mind that people seeking health care are often vulnerable and easy to manipulate. A person suffering from a serious disease has a significantly lower ability to access the content of websites critically. Furthermore, a need for a hospital often occurs in the event of emergency – unreliable information about healthcare providers can cause serious harm to vulnerable people and to society at large since there is usually no time for a critical consideration of health related information obtained from the Internet in such circumstances. This is the main reason for the highest standard of requirements for the present gTLD.

83. The GAC's comments presented by the IO indicate that the Application may be considered contrary to generally accepted legal norms relating to morality and public order. The Application does not include the specific protection safeguards listed on page 8 of the GAC's comments. The issue is not whether ICANN will follow these suggestions or not, because this Expert Panel is only expected to examine the present Application and cannot take into account possible amendments that may be made in the future. The safeguards currently employed by the Applicant - the fourteen protections required by ICANN and the eight additional that Donuts.Inc has taken on voluntarily in all its applications are in the Expert Panel view not sufficient. This conclusion is based upon GAC's concerns. The Expert Panel relies on GAC's statement since it is the body representing interests of multinational governments. Currently, .Hospital has the same level of protection as .Creditcard, .Legal or .Investments. However, in the Expert Panel's view the sensitivity of .Hospital has a different dimension than gTLDs connected with banking or legal services since human life and health require greater care than pure commercial activity.

84. The Expert Panel has also taken into consideration the possibility of conditionally upholding the Objection as long as the Applicant does not provide sufficient safeguards. However, Article 21 (d) of the Procedure states expressly: *"The remedies available to an Applicant or an Objector pursuant to any proceeding before a Expert Panel shall be limited to the success or*

dismissal of an Objection and to the refund by the DRSP to the prevailing party, as determined by the Expert Panel in its Expert Determination, of its advance payment(s) of Costs pursuant to Article 14(e) of this Procedure and any relevant provisions of the applicable DRSP Rules." Therefore, in the view of the majority of the Expert Panel such a remedy is not available in the present procedure.

85. Having carefully considered the Applicant's Application, the response to the Objection and the response to the IO's additional written statements, the Expert Panel states that the Applicant has failed to appreciate the highly sensitive nature of the applied-for string .Hospital as articulated by the IO, and the Applicant's Public Interest Commitments filed on 6 March 2013 does not in any way address the concerns of the IO.
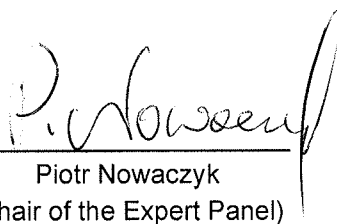
H. The great care of public health required by morality and public order is reflected in the right to health which is broadly recognized in many international law instruments

86. In this regard, the Expert Panel is convinced that the right to health is an important principle of international law, as is reflected in various documents. As it was pointed out by the IO's, Article 25 of the Universal Declaration of Human rights which provides as follows: "*Everyone has the right to a standard of living adequate for the health and well being of himself and of his family, including food, clothing, housing and medical care and necessary social services and the right to security in the event of unemployment sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control.*" Then, Article 12 (1) of the International Covenant on Economic, Social and Cultural Rights which states as follows: "*The States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.*"

87. Furthermore, the Expert Panel draws support from the 1998 European Court of Human Rights decision in the case of *Guerra* v. *Italy supra* where it was decided that a failure by the state to provide timely information on environmental pollution issues so that the citizens of that state could assess the health risks to themselves and their families was tantamount to a violation of their right to respect for their right to private and family life in breach of Article 8 of the European Convention on Human Rights. As was submitted by the IO, having access to reliable and trustworthy health related information is part of the fundament right to health. Moreover, the Expert Panel accepts the argument presented by the IO that business enterprises should respect human rights by avoiding the infringement of human rights and addressing adverse human rights impacts with which they are involved (11 principle of "Guiding Principles" that were endorsed by the United Nations Human Rights Council in its Resolution 17/4 of 16 June 2011). Accordingly, the Expert Panel finds that both states and private entities are duly bound to ensure reliable access to health related information, goods and services. And where such mechanisms for ensuring safe and reliable health related information goods and services are non-existent or inadequate then the Application breaches the right to health. The Application falls outside the scope of freedom of expression.

88. Freedom of expression is connected with special duties and responsibilities as is stated in the Guidebook. In the case of registering .Hospital those duties include an application of very specific protection and an awareness of the importance of the role of hospitals in delivering credible healthcare objectives. The Expert Panel, in considering this Application, believes that the Applicant failed to avert its mind to these responsibilities.

89. The present case is an example of a hard case which requires not only the simple application of legal rules, but also balancing different values and rules (Ronald Dworkin, Taking rights seriously, 1977). Freedom of expression and the development of services in the Internet must be balanced with the right to health and even right to life. For the majority of the Expert Panel, there is no doubt that human health and its safety tips the scale in finding the Objection to be justified.

90. The Expert Panel's decision was not taken unanimously.

VI. DECISION

91. For the foregoing reasons, in accordance with Article 21 (d) of the Procedure, the majority of the Expert Panel renders the following Expert Determination:

   (i)   The Objection is successful. Therefore, the Independent Objector is the prevailing party.

   (ii) The Centre shall refund the Independent Objector's advance payment of costs of the proceeding.

_____
Piotr Nowaczyk
(Chair of the Expert Panel)

(signature)

Ike Ehiribe
(Co-Expert of the Expert Panel)

11th December 2013.

- 20 -

August Reinisch
(Co-Expert of the Expert Panel)

(dissenting)

DATE: 11 December 2013

ATTACHMENT 6
(Decision - Dissent)

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

Dissenting Opinion
by Prof. August Reinisch
12 December 2013

relating to

THE EXPERT DETERMINATION
of 11 December 2013

issued by the Expert Panel,
composed of

Mr. Piotr Nowaczyk

Prof. August Reinisch

e-mail:
Contact Information Redacted

Contact Information Redacted

e-mail:
Contact Information Redacted

Contact Information Redacted

Mr. Ike Ehiribe
e-mail:
Contact Information Redacted

Contact Information Redacted

in Case No.
EXP/412/ICANN/29

Prof. Alain Pellet, Independent Objector (France) v. Ruby Pike, LLC (USA)

1. After having participated in an open exchange of views with my esteemed co-panelists, during which we have tried to arrive at a mutually acceptable expert determination in this case, I regret to find that this has proven impossible.

2. For the reasons outlined below, I am unable to concur with my colleagues' substantive determination to uphold the Independent Objector's (the "IO's") Objection in the case under consideration.

3. However, I am in agreement with them as regards the finding that there is no basis to assume the IO's lack of independence and impartiality, that the IO has standing in the present case and that there was no indication for a manifestly unfounded objection which would have justified a "quick look procedure".

4. I should state at the outset that I do share my co-panelists' concern about the importance of public access to reliable health-related information on the internet. However, I am unable to agree that this concern and the potential threat of future incorrect information received from websites/domains registered under the applied-for gTLD string ".hospital" constitutes a ground for upholding an objection to the registration of such a gTLD string.

5. As my colleagues have agreed, the scope of the Limited Public Interest Objection is expressly limited to the four grounds enumerated in paragraph 3.5.3. of Module 3 of the gTLD Applicant Guidebook (the "Guidebook") and "the wording of this paragraph clearly indicates that this catalogue has an exhaustive character." (Expert Determination of 11 December 2013, paras. 62, 63).

6. Pursuant to paragraph 3.5.3. of the Guidebook, "[a]n expert panel hearing a Limited Public Interest objection will consider whether the applied-for gTLD string is contrary to general principles of international law for morality and public order." These principles are contained in a number of human rights instruments which are listed in a demonstrative fashion in paragraph 3.5.3. of the Guidebook.

7. The same provision also contains an exhaustive list of four "grounds upon which an applied-for gTLD string may be considered contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law." These grounds are
    *   "Incitement to or promotion of violent lawless action;
    *   Incitement to or promotion of discrimination based upon race, colour, gender, ethnicity, religion or national origin, or other similar types of discrimination that violate generally accepted legal norms recognized under principles of international law;
    *   Incitement to or promotion of child pornography or other sexual abuse of children; or
    *   A determination that an applied-for gTLD string would be contrary to specific principles of international law as reflected in relevant international instruments of law." (paragraph 3.5.3. of the Guidebook).

8. In the present case, the IO has expressly limited his Objection to the fourth ground, i.e. he has argued that the applied-for string and its intended use would contravene "specific principles of international law as reflected in relevant international instruments of law."

9. Importantly, paragraph 3.5.3. of the Guidebook mandates that "[t]he panel will conduct its analysis on the basis of the applied-for gTLD string itself. The panel may, if needed, use as additional context the intended purpose of the TLD as stated in the application."

10. In my view the majority misconstrues the grounds for objecting to gTLDs which should be primarily the string itself and could also take into account the intended use of the string in a subsidiary way "as additional context".

11. As my co-panelists concede in the Expert Determination there is nothing in the string ".hospital" itself that is objectionable. It rather appears that, in their view, the intended use of this string is objectionable.

12. In their reasoning arriving at the result that the application is contrary to morality and public order, my co-panelists state that "[m]orality and public order require all the members of society, either public or private entities, to be extremely cautious of human life and health." (Expert Determination of 11 December 2013, para. 79). Such caution would be required because unreliable information retrieved from websites could cause serious harm to vulnerable people and to society at large.

13. Apparently this implies for the majority that the Applicant would have to ensure the veracity of content on websites registered at domains using the gTLD string ".hospital". In my co-panelists' view "the sensitivity of .Hospital has a different dimension than gTLDs connected with banking or legal services since human life and health require greater care than pure commercial activity." (Expert Determination of 11 December 2013, para. 83).

14. In concluding, the majority states that that the "Applicant has failed to appreciate the highly sensitive nature of the applied-for string .Hospital as articulated by the IO." (Expert Determination of 11 December 2013, para. 85). Thus, the Objection is held valid.

15. It is this finding that the intended purpose of the string ".hospital" by the Applicant was considered "contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law" with which I am unable to concur.

16. In my view this construction of the subsidiary relevance of the intended purpose of an applied-for string exceeds the powers of this expert panel.

17. It is not the task of an expert panel to rewrite the application standards for gTLD strings and to supplement them with higher standards in the public interest. Rather,

its task is limited to determining whether a specific applied-for string, taking into account its intended use as stated in the application is "contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law."

18. The grounds for objection listed in paragraph 3.5.3. of the Guidebook provide a clear indication that only a very limited set of particularly reprehensible behavior is objectionable. The examples listed in the Guidebook referring to the incitement or promotion of violence, unlawful discrimination and sexual abuse of children clearly illustrate this.

19. The limited scope of the fourth ground of objection in paragraph 3.5.3. of the Guidebook is also evident in the ICANN Explanatory Memorandum of 29 October 2008. Under the heading "Morality and Public Order Objection Considerations in New gTLDs" it stated that "[e]xtensive research has shown that it is difficult to identify existing generally accepted legal norms relating to morality and public order. There are, however, peremptory norms of public international law from which no derogation is permitted and which can be modified only by a subsequent norm of international law having the same character (jus cogens), such as the prohibition of the use of force, the law of genocide, the principle of racial non-discrimination, crimes against humanity and the rules prohibiting piracy and trade in slaves." (ICANN, New gTLD Program Explanatory Memorandum, p. 3, available at http://archive.icann.org/en/topics/new-gtlds/morality-public-order-draft-29oct08-en.pdf). This implies that only certain particularly reprehensive acts and omissions constitute grounds for objection.

20. This concept was taken up by the IO in stating his mission as one of protecting against the promotion of seriously offensive behavior. According to the IO, "the essential criterion is not to determine whether or not the application is contrary to the multiple potential interests of the public who use the global Internet. It is not the mission of the Independent Objector to protect personal or commercial interests of individual Internet users. The limited public interest objection aims at ensuring that no applied-for gTLD string and its intended use is contrary to fundamental norms of public order and morality that are recognized under international law." (Website of the Independent Objector, http://www.independent-objector-newgtlds.org/).

21. The IO also provides an illustration of the limited scope of objectionable application by stating that "a limited public interests objection could be triggered in case an application promote unlawful activities or international crimes, such as child pornography, sale of counterfeit medicines, slavery, torture or genocide; in case it endangers international public order or again in case it is obviously against moral values that have been transcribed in international norms." (Website of the Independent Objector, http://www.independent-objector-newgtlds.org/).

22. As stated in paragraph 3.5.3. of the Guidebook, in order to take the intended use into account, the IO and the Panel of Experts are required to look at the application itself.

23. Applying these considerations to the present case, one may well consider that the application for a string ".hospital" which contains an indication that the intended purpose of such a string might be the sale of counterfeit medicine or maybe also the offering of unsafe medical treatment or other high risk medical services might be objectionable.

24. However, I fail to see that the application by the Applicant indicates any intention of inciting or promoting any such highly reprehensive behavior.

25. The Applicant is a commercial domain name provider who intends to offer domain sites with the gTLD string ".hospital". It is the task of such a provider to ensure that domains are available and functioning and that specific users may register. The prospective domain name provider in the present case is not itself active in the health or medical field and there is nothing in the application that lends itself to presume that it intends to engage in any activities like the sale of medicine, the offering of medical treatment or other medical or hospital services, let alone in the sale of counterfeit medicine or other reprehensible behavior.

26. Thus, under the IO's own standards it would appear difficult to image how the present application could be considered to be contrary to "fundamental norms of public order and morality that are recognized under international law."

27. One may criticize that Applicant's purpose is primarily commercial, regarding the applied-for gTLD string as mere "commodity", but that does not render it contrary to "morality and public order".

28. I am sympathetic with the majority's concern that the lack of a specific guarantee that the Applicant will ensure that the information imparted through internet sites registered with the ".hospital" gTLD will be reliable and trustworthy information is problematic.

29. However, I cannot tell from the current ICANN registration prerequisites that such an implied substantive, content-wise check is a precondition for a gTLD string registration.

30. The majority relies heavily on the fact that the present application "does not include those specific protection safeguards listed at page 8 of the GAC's comments." (Expert Determination of 11 December 2013, para. 83). Indeed, on 11 April 2013, ICANN's Governmental Advisory Committee (GAC) issued an Advice to the ICANN Board which stated that extensive additional safeguards should be put in place for a whole range of gTLDs including ".hospital". (Available at http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm).

31. The recommended safeguards comprise for all new gTLDs: (i) increased WHOIS verification and checks; (ii) expanded terms of use by registry operators to mitigate abusive activity; (iii) increased security checks by registry operators, (iv) constant record keeping by registry operators to identify frequent inaccurate WHOIS records and security threats; (v) provision of mechanisms for the handling of complaints by registry operators arising from the provision of inaccurate WHOIS information or

the facilitation of infringement activity contrary to applicable law; and (vi) the identification of real and immediate consequences for providing inaccurate WHOIS information and engaging in infringement or unlawful activity.

32. In addition, the GAC recommended safeguards for new gTLDs carrying a higher risk of consumer harm, which include the string ".hospital", such as: (i) heightened use policy requirements in the interest of consumers, (ii) information obligations of registrars in this request, (iii) security measures for sensitive health and financial data, (iv) strategies to mitigate fraud and other illegal activities, and (v) the establishment by registrants of single points of contact for complaints.

33. I agree with my co-panelists that "the issue is not whether ICANN will follow these suggestions or not because this Panel is only expected to examine the present Application and cannot take into account possible amendments that may be made in the future." (Expert Determination of 11 December 2013, para. 83).

34. However, I feel compelled to conclude that as long as ICANN has not adopted these GAC recommendations and added specific additional requirements for applications relating to the health sector, it would be inappropriate to demand compliance with such recommendations from applicants in order to grant gTLDs.

35. This consideration is all the more relevant to the function of the Expert Panel whose task is limited to ensuring that gTLD names, taking into account their intended use, are not contrary to "fundamental norms of public order and morality that are recognized under international law". It is not the Expert Panel's assignment to check compliance with registration prerequisites.

36. While I agree with my colleagues that "a hard case […] requires not only the simple application of legal rules, but also the balancing of different values and rules" (Expert Determination of 11 December 2013, para. 89), I do not think that this would entitle us to rewrite ICANN's current registration policy and usurp its registration role.

37. Consequently, I have to dissent and would reject the IO's Objection. I cannot see that the IO has met the burden of proof establishing that the intended purpose of the Applicant for the gTLD string ".hospital" as stated in its application is contrary to "fundamental norms of public order and morality that are recognized under international law."

_____
August Reinisch

(12 December 2013)

ATTACHMENT 7
(Ruby Pike Request for Additional Submission re GAC Advice)

From: Don Moody
Sent:

Cc:
Subject: RE: EXP/412/ICANN/29 - IO v. Ruby Pike - .HOSPITAL
Attachments: Annex A.pdf; Annex B.pdf

Dear ICC, Expert Panel, Parties and Counsel:

Applicant respectfully submits the following information to update the Panel regarding matters raised in
the Objection and further submissions made by the Objector.

Among other things, Objector has argued that the Application runs contrary to general principles of
international law for morality and public order due to an alleged lack of the types of safeguards
proposed by the GAC in its Beijing Communiqué of April 2013. Please be advised that, per the attached
Annex A -- copy also available at:
https://www.icann.org/en/news/correspondence/crocker-to-dryden-3-29oct13-en.pdf -- ICANN has formally announced its intention to adopt the "GAC's Beijing
Communiqué advice concerning Category 1 and Category 2 Safeguards," which the GAC responded to in
a follow-up communiqué issued during the recently-conducted meetings in Buenos Aires. See Annex B
and http://www.icann.org/en/news/correspondence/gac-to-board-20nov13-en.pdf.

To the extent ICANN has so adopted the GAC advice, Applicant must implement the safeguards, if
awarded the subject string, as a term of its registry agreement with ICANN for the string. Applicant
therefore respectfully submits that, to the extent Objector claims any contravention of international
morality or public order legal principles based on Applicant's alleged lack of GAC-recommended
safeguards, ICANN's recent action has rendered that portion of the Objection moot, and eliminates it as
a basis for denying Applicant its presumptive right to compete for and, if awarded, operate the string.

Sincerely,

Don C. Moody, J.D., M.S.
New gTLD Disputes
Registered USPTO

ANNEX A

[Letter from Stephen D. Crocker, Chair, ICANN Board of Directors to Heather Dryden, Chair, Governmental Advisory Committee, dated October 29, 2013]

ICANN

29 October 2013

Heather Dryden
Chair, Governmental Advisory Committee

Re: NGPC Consideration of GAC Category 1 and Category 2 Safeguard Advice

Dear Heather,

On behalf of the New gTLD Program Committee, I am pleased to inform you that the NGPC is intending to accept the GAC's Beijing Communiqué advice concerning Category 1 and Category 2 Safeguards. Attached please find documents that describe how ICANN intends to implement the advice. A summary of the implementation plans appears below.

Category 1 Safeguards

The text of the Category 1 Safeguards have been modified as appropriate to meet the spirit and intent of the advice in a manner that allows the requirements to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement ("PIC Spec"). The PIC Spec and a rationale explaining the modifications are attached.

The implementation plan also distinguishes the list of TLD strings listed in the Category 1 safeguard advice between strings that the NGPC considers strings associated with market sectors or industries that have highly regulated entry requirements in multiple jurisdictions, and those that do not. The Category 1 Safeguards in the PIC Spec will apply to the TLD strings based on how the TLD string is categorized. The list of re-categorized Category 1 strings is attached.

Category 2 Safeguards

ICANN contacted the 186 applicants for strings identified in the GAC's Category 2 safeguard advice. The applicants were asked to respond by a specified date indicating whether the applied-for TLD will be operated as an exclusive access registry. An overwhelming majority of the applicants (174) indicated that the TLD would not be operated as an exclusive access registry. The NGPC recently adopted a resolution directing staff to move forward with the contracting process for applicants for strings identified in the Category 2 Safeguards that were prepared to enter into the Registry Agreement as approved, since moving forward with these applicants was consistent with the GAC's advice.

Ten applicants responded that the TLD would be operated as an exclusive access registry. These 10 applicants have applied for the following strings: .BROKER, .CRUISE, .DATA, .DVR, .GROCERY, .MOBILE, .PHONE, .STORE, .THEATER, .THEATRE and .TIRES. The NGPC directed staff to prepare an analysis and proposal to implement the Category 2 safeguard advice for these applicants. Staff requested the applicants to provide an explanation of how the proposed exclusive registry access serves a public interest goal. When available, the responses will be forwarded to the NGPC and the GAC for further consideration.

I hope this information is helpful. I look forward to seeing you at the ICANN 48 Meeting in Buenos Aires.

Best regards,

Stephen D. Crocker
Chair, ICANN Board of Directors

Category 1 Safeguards as Public Interest Commitments in Specification 11 of the New gTLD Registry Agreement

1. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring registrants to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

2. Registry operators will include a provision in their Registry-Registrar Agreements that requires registrars at the time of registration to notify registrants of the requirement to comply with all applicable laws.

3. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

4. Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self-regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication, including for the purpose of facilitating the development of a strategy to mitigate the risks of fraudulent and other illegal activities.

5. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to provide administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

6. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.

7. If a Registry Operator receives a complaint expressing doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents regarding the authenticity.

8. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision

requiring Registrants to report any material changes to the validity of the Registrants' authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

9. Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.

GAC Category 1 Safeguard Advice
Rationale for Changes to Safeguard Language in the PIC Spec

The NGPC intends to adapt the language of the Category 1 safeguards to meet the spirit and intent of the GAC's Category 1 Safeguard Advice in a manner that allows the safeguards to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement (the "Category 1 PIC Spec").

Safeguards #1, #2 and #5

Because registry operators and ICANN do not have contractual relationships with registrants, additional language was added to Safeguards #1, #2 and #5 to refer to Registry-Registrar Agreements and Registration Agreements to impose the obligation on registrants required in the safeguard advice.

Safeguard #3

Safeguard #3 would require registrants to implement reasonable and appropriate security measures if the registrant collects and maintains sensitive health and financial data. The security measures should be commensurate with the offering of those services, as defined by applicable law and recognized industry standards. The NGPC notes that implementation would not be possible because it is not clear how "recognized industry standards" would be identified and applied in the context of hundreds of different sectors.

The language in the PIC Spec to address this safeguard was adapted to require that the security measures are commensurate with the offering of those services, as defined by applicable law.

Safeguard #4

The NGPC notes that the safeguard raises contract enforcement questions (e.g., how are the relevant regulatory agencies and industry self-regulatory organizations identified; who determines which industry self-regulation organizations bodies are "relevant" to a particular string and which governmental body is the competent regulatory agency). Additionally, some regulatory bodies or industry self-regulatory bodies may not be responsive to collaboration with registry operators.

To address these concerns, the safeguard language in the PIC Spec was drafted in a way to avoid a situation where the registry operator would be in breach of the registry agreement if regulatory body won't agree to a relationship with the registry operator.

Safeguards #6, #7 and #8

The implementation of safeguards #6-8 would change the nature of some new gTLDs from being open to uses that are not regulated into restricted TLDs open only to registrants that can prove their status or credentials. The NGPC also notes that implementation would potentially discriminate against users in developing nations whose governments do not have regulatory bodies or keep databases which a registry/registrar could work with to verify credentials, and would potentially discriminate against users in developed nations whose governments have developed different regulatory regimes.

The language in the Category 1 PIC Spec was modified to address these concerns. As an initial matter, the registrant would be required to make an attestation that the registrant possesses any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD string. The registrant is also required to report any material changes to the validity of their authorizations. This provision provides the registrant the opportunity to provide this information because it is better positioned to

If the registry operator receives complaints about the authenticity of the licenses or credentials, the registry operator is obligated to consult with the relevant national supervisory authorities, or their equivalents regarding the authenticity.

GAC Category 1 Strings

Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-3 applicable)	Highly-regulated Sectors/Closed Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-8 applicable)
Children: .kid, .kids, .kinder, .game, .games, .juegos, .play, .school, .schule, toys	
Environmental: .earth, .eco, .green, .bio, .organic	
Health and Fitness: .care, .diet, .fit, .fitness, .health, .heart, .hiv, .rehab, .clinic, .healthy (IDN Chinese equivalent), .dental, .physio, .healthcare, .med, .organic, .doctor	**Health and Fitness:** pharmacy, .surgery, .dentist , .dds, , .hospital, .medical
Financial: capital, . cash, .cashbackbonus, .broker, .brokers, .claims, .exchange, .finance, .financial, .forex, .fund, .investments, .lease, .loan, .loans, .market, . markets, .money, .pay, .payu, .retirement, .save, .trading, .credit, .insure, .netbank, .tax, .travelersinsurance, .financialaid, .vermogensberatung, .mortgage, .reit	**Financial:** .bank, .banque, .creditunion, .creditcard, .insurance, .ira, .lifeinsurance, .mutualfunds, .mutuelle, .vermogensberater, and .vesicherung, .autoinsurance, .carinsurance
	Gambling: .bet, .bingo, .lotto, .poker,.spreadbetting, .casino
Charity: .care, .gives, .giving	**Charity:** .charity (and IDN Chinese equivalent)
Education: .degree, .mba	**Education:** .university
Intellectual Property: .audio, .book (and IDN equivalent), .broadway, .film, .game, .games, .juegos, .movie, .music, .software, .song, .tunes,	

Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-3 applicable)	Highly-regulated Sectors/Closed Entry Requirements in Multiple Jurisdictions (Category 1 Safeguards 1-8 applicable)
.fashion (and IDN equivalent), .video, .app, .art, .author, .band, .beats, .cloud (and IDN equivalent), .data, .design, .digital, .download, .entertainment, .fan, .fans, .free, .gratis, .discount, .sale, .hiphop, .media, .news, .online, .pictures, .radio, .rip, .show, .theater, .theatre, .tour, .tours, .tvs, .video, .zip	
Professional Services: .accountant, .accountants, .architect, .associates, .broker, .brokers, .engineer, .legal, .realtor, .realty, .vet, .doctor, .engineering, .law	**Professional Services:** .abogado, .attorney, .cpa, .dentist, .dds, .lawyer.
Corporate Identifiers: .limited	**Corporate Identifiers:** .corp, .gmbh, .inc, .llc, .llp, .ltda, .ltd, .sarl, .srl, .sal
Generic Geographic Terms: .capital .town, .city	
.reise, .reisen .weather	

Special Safeguards Required

Inherently Governmental Functions:
.army, .navy, .airforce
Potential for Cyber Bullying/Harassment:
.fail, .gripe, .sucks, .wtf

Category 1 Safeguards as Public Interest Commitments in Specification 11 of the New gTLD Registry Agreement

1. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring registrants to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

2. Registry operators will include a provision in their Registry-Registrar Agreements that requires registrars at the time of registration to notify registrants of the requirement to comply with all applicable laws.

3. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

4. Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self-regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication, including for the purpose of facilitating the development of a strategy to mitigate the risks of fraudulent and other illegal activities.

5. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to provide administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

6. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring a representation that the Registrant possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string.

7. If a Registry Operator receives a complaint expressing doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents regarding the authenticity.

8. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring Registrants to report any material changes to the validity of the Registrants' authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the Registry TLD string in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

9. Registry Operator will develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.

ANNEX B

[GAC Buenos Aires Communiqué, dated November 20, 2013]

Governmental Advisory Committee

Buenos Aires, 20 November 2013

GAC Communiqué – Buenos Aires, Argentina

I. Introduction

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Buenos Aires during the week of 16 November 2013. 56 GAC Members attended the meetings, with one GAC Member participating remotely, and five Observers. The GAC expresses warm thanks to the local host, NIC Argentina, for their support.

At the beginning of its meeting the GAC expressed its sympathy for and solidarity with the people and government of the Philippines following the recent disaster of Typhoon Haiyan.

II. GAC Advice to the Board[1]

1. Category 1 and Category 2 Safeguard Advice

The GAC welcomed the response of the Board to the GAC's Beijing Communiqué advice on Category 1 and Category 2 safeguards. The GAC received useful information regarding implementation of the safeguards during its discussions with the New gTLD Program Committee. GAC members asked for clarification of a number of issues and look forward to ICANN's response.

a. The GAC highlights the importance of its Beijing advice on 'Restricted Access' registries, particularly with regard to the need to avoid undue preference and/or undue disadvantage.

   i. **The GAC requests**

      1. A briefing on whether the Board considers that the existing PIC specifications (including 3c) fully implements this advice.

b. The GAC requests a briefing on the public policy implications of holding auctions to resolve string contention (including community applications).

---

[1] To track the history and progress of GAC Advice to the Board, please visit the GAC Advice Online Register available at: https://gacweb.icann.org/display/GACADV/GAC+Register+of+Advice

c. The GAC considers that new gTLD registry operators should be made aware of the importance of protecting children and their rights consistent with the UN Convention on the Rights of the Child.

d. **The GAC advises the ICANN Board:**

   i. to re-categorize the string .doctor as falling within Category 1 safeguard advice addressing highly regulated sectors, therefore ascribing these domains exclusively to legitimate medical practitioners. The GAC notes the strong implications for consumer protection and consumer trust, and the need for proper medical ethical standards, demanded by the medical field online to be fully respected.

e. The GAC welcomes the Board's communication with applicants with regard to open and closed gTLDs, but seeks **written clarification** of how strings are identified as being generic.

2. **GAC Objections to Specific Applications (ref. Beijing Communiqué 1.c.)**

   a. **.guangzhou (IDN in Chinese), .shenzhen (IDN in Chinese), and .spa**

      Discussions between interested parties are ongoing so as noted in the Durban Communiqué

      i. **The GAC advises the ICANN Board**:

         1. Not to proceed beyond initial evaluation until the agreements between the relevant parties are reached.

            a. The application for .guangzhou (IDN in Chinese – application number 1-1121-22691)

            b. The application for .shenzhen (IDN in Chinese – 1-1121-82863)

            c. The applications for .spa (application number 1-1309-12524 and 1-1619-92115)

   b. The GAC notes that the application for .yun (application number 1-1318-12524) has been withdrawn.

   c. The GAC welcomes the Board's acceptance of its advice in the Durban Communiqué on the application for .thai.

   d. The GAC sought an update from the Board on the current status of the implementation of the GAC Advice for .amazon.

3. **.wine and .vin**

   The GAC took note of the developments on the two strings .wine and .vin from its previous meetings in Beijing and Durban.

   GAC members have undertaken extensive discussions to examine a diversity of views on these applications, and the protections associated with Geographical Indications (GIs).

GAC considers that appropriate safeguards against possible abuse of these new gTLDs are needed.

Some members are of the view, after prolonged and careful consideration, that the existing safeguards outlined in the GAC's Beijing Communiqué and implemented by the ICANN Board are appropriate and sufficient to deal with the potential for misuse of the .wine and .vin new gTLDs. These members welcome the Board's response to these safeguards, which prohibit fraudulent or deceptive use of domain names. They consider that it would be inappropriate and a serious concern if the agreed international settings on GIs were to be redesigned by ICANN. The current protections for geographical indications are the outcome of carefully balanced negotiations. Any changes to those protections are more appropriately negotiated among intellectual property experts in the World Intellectual Property Organization and the World Trade Organization.

Other members consider that delegation of .wine and.vin strings should remain on hold until either sufficient additional safeguards to protect GIs are put into place in these strings to protect the consumers and businesses that rely on such GIs; or common ground has been reached for the worldwide protection of GIs via international fora and wide array of major trade agreements. Given this changing context, they welcome the current face-to-face talks between the applicants for .wine and .vin. and wine producers, aiming to protect their assets and consumers' interests whilst taking into account governments' public policy concerns.

The Board may wish to seek a clear understanding of the legally complex and politically sensitive background on this matter in order to consider the appropriate next steps in the process of delegating the two strings. GAC members may wish to write to the Board to further elaborate their views.

4. **Protection of Inter-Governmental Organisations (IGOs)**

    a. **The GAC Advises the ICANN Board that:**

        i. The GAC, together with IGOs, remains committed to continuing the dialogue with NGPC on finalising the modalities for permanent protection of IGO acronyms at the second level, by putting in place a mechanism which would:

            1. provide for a permanent system of notifications to both the potential registrant   and the relevant IGO as to a possible conflict if a potential registrant seeks to register a domain name matching the acronym of that IGO;

            2. allow the IGO a timely opportunity to effectively prevent potential misuse and confusion;

            3. allow for a final and binding determination by an independent third party in order to resolve any disagreement between an IGO and a potential registrant; and

            4. be at no cost or of a nominal cost only to the IGO.

The GAC looks forward to receiving the alternative NGPC proposal adequately addressing this advice. The initial protections for IGO acronyms should remain in place until the dialogue between the NGPC, the IGOs and the GAC ensuring the implementation of this protection is completed.

5. **Special Launch Program for Geographic and Community TLDs**

The GAC recognizes the importance of the priority inclusion of government and locally relevant name strings for the successful launch and continued administration of community and geographic TLDs.

The GAC appreciates that the Trademark Clearing House (TMCH) is an important rights protection mechanism applicable across all the new gTLDs and has an invaluable role to fulfill across the new gTLD spectrum as a basic safety net for the protection of trademark rights.

   a. **The GAC Advises the ICANN Board:**

      i. that ICANN provide clarity on the proposed launch program for special cases as a matter of urgency.

6. **Protection of Red Cross/Red Crescent Names**

   a. **The GAC advises the ICANN Board:**

      i. that it is giving further consideration to the way in which existing protections should apply to the words "Red Cross", "Red Crescent" and related designations at the top and second levels with specific regard to national Red Cross and Red Crescent entities; and that it will provide further advice to the Board on this.

7. **.islam and .halal**

   a. GAC took note of letters sent by the OIC and the ICANN Chairman in relation to the strings .islam and .halal. The GAC has previously provided advice in its Beijing Communiqué, when it concluded its discussions on these strings. The GAC Chair will respond to the OIC correspondence accordingly, noting the OIC's plans to hold a meeting in early December. The GAC chair will also respond to the ICANN Chair's correspondence in similar terms.

III. Inter-constituencies Activities

1. **Meeting with the Generic Names Supporting Organisation (GNSO)**

The GAC met with the GNSO and welcomed preliminary work that has been done to identify improved ways for earlier GAC involvement in policy development processes which have potential public policy aspects. A joint GAC/GNSO working group will be established to develop inter-sessionally more detailed options for implementation.

2. **Meeting with the Expert Working Group on gTLD Directory Services (EWG)**

The GAC met with the EWG and exchanged views on the model proposed by the EWG for next generation directory services. GAC members highlighted a range of issues including the importance of applicable data privacy laws, the balance between public and restricted data elements, and the accreditation process to allow access to restricted data for legitimate purposes. The GAC welcomed the opportunity for continuing engagement with the EWG.

3. **Meeting with the Country Code Names Supporting Organisation (ccNSO)**

The GAC met with the ccNSO and received briefings on ccNSO working groups on the IDN policy development process and the framework of interpretation; and the study group on country names. The GAC committed to continuing engagement with these issues, all of which have public policy implications, and will continue to work closely with the ccNSO.

4. **Meeting with the Accountability and Transparency Review Team 2 (ATRT 2)**

The GAC is grateful for the work undertaken by the ATRT2 and discussed with review team members their draft recommendations and report, noting that it was valuable to gain an external perspective on the work and operations of the GAC. The GAC has already made progress in relation to early engagement in policy development processes, increased transparency and improved working methods, but acknowledges that there is always more to be done, particularly in outreach. GAC members noted that the GAC provides policy advice, not legal advice. The GAC noted that each member already operates within their own government's code of conduct framework.

5. **Meeting with the Brand Registry Group (BRG)**

The GAC met with the Brand Registry Group to discuss their proposal for a streamlined process under an addendum to the Registry Agreement for the approval of country names and 2-letter and character codes at the second level. The GAC undertook to consider this proposal further and respond to the BRG in due course.

***

The GAC warmly thanks the GNSO, the EWG, the ccNSO, and the ATRT 2, who jointly met with the GAC; as well as all those among the ICANN community who have contributed to the dialogue with the GAC in Buenos Aires.

IV. Internal Matters

1. **New Members and Observers** - The GAC welcomes the Commonwealth of Dominica and Montenegro as members, and the Organisation of Islamic Cooperation and the Caribbean Telecommunications Union as observers.

2. **GAC Secretariat** – The independent consultants, Australian Continuous Improvement Group, have begun providing additional secretariat services to the

GAC. A range of measures to improve the efficiency and effectiveness of the GAC is being progressively implemented.

3. **GAC Leadership** - The GAC welcomed the re-election of the current Vice Chairs (Australia, Switzerland and Trinidad and Tobago) for a further term. The issue of a possible increase in the number of Vice Chairs to better represent regions and manage workload has been referred to the GAC working group on working methods for consideration and report.

4. **New gTLDs** - At the ICANN meeting in Durban, the GAC formed a working group to begin consideration of potential public policy input for future rounds of new gTLDs. This working group has been focusing on issues associated with the protection of geographic names, the processes associated with identified communities, and developing economy issues and applicant support. The outcomes of the Geographic names working group are expected to be presented to the community by the ICANN 49 Singapore meeting. The GAC looks forward to discussing these issues with the community in future meetings.

5. **Working Methods** – At the ICANN meeting in Durban the GAC formed a working group to consider improvements to the GAC's working methods. A range of immediate measures has been identified and is being progressively implemented. Other matters will be progressed in coordination with related initiatives including the ATRT 2 process.

6. **High Level Meeting** - A high level meeting of governments will be held in London in June 2014 in conjunction with the ICANN and GAC meetings. The agenda for the meeting should be finalised in Singapore.

V.   Next Meeting

The GAC will meet during the period of the 49th ICANN meeting in Singapore.

ATTACHMENT 8
(IO Response to Ruby Pike Request for Additional Submission re GAC Advice)

Dear Expert Panel,

I am writing in response to Mr Moody's mail received on 4 December 2013.

I note that, pursuant to Article 17 (a) of the attachment to Module 3 of the Applicant Guidebook, New gTLD Dispute Resolution Procedure (hereinafter "the Procedure"), "the Panel may decide whether the parties shall submit any written statements in addition to the Objection and the Response, and it shall fix time limits for such submissions". I therefore request the Expert Panel to dismiss this unsolicited additional statement which was not submitted in accordance with the Procedure.

Should the Expert Panel accept this new submission, I wish to prevail myself of the right to respond in accordance with Article 4 of the Procedure, which stipulates that the Expert Panel shall "ensure that the parties are treated with equality, and that each party is given a reasonable opportunity to present its position".

In any case, I wish to emphasize that in its authorized additional written statement, the Applicant submitted that "because ICANN, as Objector points out, already is considering such GAC advice in the appropriate process, the Panel need not concern itself with such policy discussion" and that "the GAC's policy recommendations have no relevance to these objection proceedings." Obviously, instead of strengthening the Applicant's previous submission, this new email highlights its lack of incoherence and consistency.

Sincerely,

Alain PELLET
ICANN - Independent Objector

Le 4 déc. 2013 à 05:37, "Don Moody" Contact Information Redacted a écrit :

Dear ICC, Expert Panel, Parties and Counsel:

Applicant respectfully submits the following information to update the Panel regarding matters raised in the Objection and further submissions made by the Objector.

Among other things, Objector has argued that the Application runs contrary to general principles of international law for morality and public order due to an alleged lack of the types of safeguards proposed by the GAC in its Beijing Communiqué of April 2013. Please be advised that, per the attached Annex A -- copy also available at: https://www.icann.org/en/news/correspondence/crocker-to-dryden-3-29oct13-en.pdf -- ICANN has formally announced its intention to adopt the "GAC's Beijing Communiqué advice concerning Category 1 and Category 2 Safeguards," which the GAC responded to in a follow-up communiqué issued during the recently-conducted meetings in Buenos Aires. See Annex B and http://www.icann.org/en/news/correspondence/gac-to-board-20nov13-en.pdf.

To the extent ICANN has so adopted the GAC advice, Applicant must implement the safeguards, if awarded the subject string, as a term of its registry agreement with ICANN for the string. Applicant therefore respectfully submits that, to the extent Objector claims any contravention of international morality or public order legal principles based on Applicant's alleged lack of GAC-recommended safeguards, ICANN's recent action has rendered that portion of the Objection moot, and eliminates it as a basis for denying Applicant its presumptive right to compete for and, if awarded, operate the string.

Sincerely,

Don C. Moody, J.D., M.S.
New gTLD Disputes
Registered USPTO

<Annex A.pdf>
<Annex B.pdf>

ATTACHMENT 9
(ICC Correspondence on Ruby Pike Request for Additional Submission re GAC Advice)

Sent: Wednesday, December 11, 2013 10:12 AM
To: 'Alain Pellet'; Don Moody; John M. Genga
Cc: Contact Information Redacted

Contact Information Redacted

Subject: RE: EXP/412/ICANN/29 - IO v. Ruby Pike - .HOSPITAL

Dear Sirs,

The Centre acknowledges receipt of Mr. Don Moody's e-mail of 4 December 2013, sent on behalf of the Applicant, a copy of which was sent to the Independent Objector and the Expert Panel directly.

The Centre further acknowledges receipt of Mr. Alain Pellet, Independent Objector's e-mail of 5 December 2013, a copy of which was sent to the Applicant and to the Expert Panel directly.

The Centre would like to draw your attention to the fact that ICANN's New gTLD Dispute Resolution Procedure does not provide for any specific provision regarding the issue raised by the Applicant. Accordingly, the Centre has referred the decision of whether to take the Applicant's additional information into account to the Expert Panel.

Further, the Centre acknowledges receipt of the Expert Panel's e-mail of 11 December 2013, in which the Expert Panel indicated that the submissions were not taken into account.

Please also be informed that the draft Expert Determination as submitted by the Expert Panel to the Centre will be notified to you shortly.

Please do not hesitate to contact us if you have any further questions,

Best regards,

Špela Košak

Špela Košak | Deputy Manager
NB: New address since 21 October 2013!
International Centre for ADR | International Chamber of Commerce
Contact Information Redacted

1st ICC International Mediation Round Table: 6 February 2014
9th ICC International Commercial Mediation Competition: 7 – 12 February 2014
1st ICC Workshop on new Mediation Rules: 17 September 2014
5th ICC International Mediation Conference: 18 September 2014

From: Alain Pellet [mailto:contact@independent-objector-newgtlds.org]
Sent: Thursday, December 05, 2013 10:21 PM
To: Don Moody; Magdalena Lackoronska; REINISCH August; EHIRIBE Ike
Cc: Contact Information Redacted
                 Contact Information Redacted
          Contact Information Redacted
Subject: Re: EXP/412/ICANN/29 - IO v. Ruby Pike - .HOSPITAL

Dear Expert Panel,
I am writing in response to Mr Moody's mail received on 4 December 2013.
I note that, pursuant to Article 17 (a) of the attachment to Module 3 of the Applicant Guidebook, New gTLD Dispute Resolution Procedure (hereinafter "the Procedure"), "the Panel may decide whether the parties shall submit any written statements in addition to the Objection and the Response, and it shall fix time limits for such submissions". I therefore request the Expert Panel to dismiss this unsolicited additional statement which was not submitted in accordance with the Procedure.
Should the Expert Panel accept this new submission, I wish to prevail myself of the right to respond in accordance with Article 4 of the Procedure, which stipulates that the Expert Panel shall "ensure that the parties are treated with equality, and that each party is given a reasonable opportunity to present its position".
In any case, I wish to emphasize that in its authorized additional written statement, the Applicant submitted that "because ICANN, as Objector points out, already is considering such GAC advice in the appropriate process, the Panel need not concern itself with such policy discussion" and that "the GAC's policy recommendations have no relevance to these objection proceedings." Obviously, instead of strengthening the Applicant's previous submission, this new email highlights its lack of incoherence and consistency.
Sincerely,
Alain PELLET
ICANN - Independent Objector

Le 4 déc. 2013 à 05:37, "Don Moody" Contact Information Redacted a écrit :

Dear ICC, Expert Panel, Parties and Counsel:

Applicant respectfully submits the following information to update the Panel regarding matters raised in the Objection and further submissions made by the Objector.

Among other things, Objector has argued that the Application runs contrary to general principles of international law for morality and public order due to an alleged lack of the types of safeguards proposed by the GAC in its Beijing Communiqué of April 2013. Please be advised that, per the attached Annex A -- copy also available at:
https://www.icann.org/en/news/correspondence/crocker-to-dryden-3-29oct13-en.pdf -- ICANN has formally announced its intention to adopt the "GAC's Beijing Communiqué advice

concerning Category 1 and Category 2 Safeguards," which the GAC responded to in a follow-up communiqué issued during the recently-conducted meetings in Buenos Aires. See Annex B and http://www.icann.org/en/news/correspondence/gac-to-board-20nov13-en.pdf.

To the extent ICANN has so adopted the GAC advice, Applicant must implement the safeguards, if awarded the subject string, as a term of its registry agreement with ICANN for the string. Applicant therefore respectfully submits that, to the extent Objector claims any contravention of international morality or public order legal principles based on Applicant's alleged lack of GAC-recommended safeguards, ICANN's recent action has rendered that portion of the Objection moot, and eliminates it as a basis for denying Applicant its presumptive right to compete for and, if awarded, operate the string.

Sincerely,

Don C. Moody, J.D., M.S.
New gTLD Disputes
Registered USPTO
Contact Information Redacted

<Annex A.pdf>
<Annex B.pdf>