crowell moring

Annex 1.

Despegar Online SRL
Contact Information
Redacted

Ms. Lillian Fosteris and Mr. Taylor Frank
Contact Information Redacted

Spring McCook, LLC
Contact Information
Redacted

Donuts Inc.
Contact Information
Redacted

Mr. Jon Nevett
Contact Information Redacted

Famous Four Media Limited
Contact Information Redacted

Mr. Peter Young and Mr. Geir Rasmussen
Contact Information Redacted

Fegistry LLC
Contact Information Redacted

Mr. Jay Westerdal
CEO
Contact Information Redacted

Radix FZC
Contact Information Redacted

Ms. Shweta Sahjwani
Contact Information Redacted

crowell moring

Annex 2.

New gTLD Application Submitted to ICANN by: Despegar Online SRL

String: HOTEL

Originally Posted: 13 June 2012

Application ID: 1-1249-36568

Applicant Information

1. Full legal name

Despegar Online SRL

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

http://www.despegar.com

Primary Contact

6(a). Name

Joshua Bourne

6(b). Title

Managing Partner

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

Martín Rastellino

7(b). Title

President

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

Corporation

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

Montevideo, Uruguay

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.

SATYLCA S.A.

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

Martín Rastellino	President

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

Alejandro Tamer	Vice President South America & Marketing
Christian Vilate	Vice President Hotels
Edgardo Sokolowicz	Chief Information Officer
Mariano Fiori	Vice President Administration & Finance
Martín Rastellino	President & Chief Operating Officer
Roberto Souviron	Chief Executive Officer

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

SATYLCA S.A.	Not Applicable

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

Applied-for gTLD string

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

HOTEL

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.

Despegar Online SRL foresees no known rendering issues in connection with the proposed .HOTEL gTLD for which it is applying. This answer is based upon consultation with Despegar's selected back-end provider, Neustar, which has successfully launched a number of new gTLDs over the last decade. In reaching this determination, Neustar analyzed the following data:

-ICANN's Security Stability Advisory Committee (SSAC) entitled Alternative TLD Name Systems and Roots: Conflict, Control and Consequences (SAC009);
-IAB - RFC3696 "Application Techniques for Checking and Transformation of Names"
-Known software issues which Neustar has encountered during the last decade launching new gTLDs;
-Character type and length;
-ICANN supplemental notes to Question 16; and
-ICANN's presentation during its Costa Rica regional meeting on TLD Universal Acceptance.

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.

18.1 Mission and Purpose of .HOTEL

Despegar Online SRL ("Despegar") is a leading multinational tourism organization and a branch of the largest online travel agency in Latin America. Despegar enables customers to book airline tickets, hotel rooms, rental cars, vacation packages, and other travel-related services. Despegar also powers travel bookings for various airlines, hotels, rental car agencies, and other tourism-related organizations internationally. Despegar serves more than five million clients annually and has a presence in 21 countries. Its services and online content are accessible in the .COM gTLD and various ccTLDs.

Despegar is applying for five generic-term gTLDs: .VUELOS and .HOTELES, which target its Spanish-speaking audiences; .PASSAGENS and .HOTEIS, which target its Portuguese-speaking audiences; and .HOTEL, which targets its English, Spanish, and Portuguese-speaking audiences.

The intended future mission and purpose of the .HOTEL gTLD is to serve as a

trusted, hierarchical, secure, and intuitive namespace provided by Despegar for its global audience. At present, such a dedicated, secure namespace does not exist; Despegar believes that consumers and travel-related companies will benefit from the presence of a targeted and dedicated secure portal. Despegar is applying for .HOTEL, but at the time of filing this application, there has not been enough time, and there is not enough market information available, to fully analyze and evaluate all potential use case options.

Despegar will be analyzing other gTLD applications and general market adoption to determine potential use case options to most effectively serve and enhance its online strategy as a leading provider of travel services. Despegar helps customers in many parts of the world book various travel reservations and aims to protect its customers and other Internet users from fraudulent information. The .HOTEL gTLD will accord with the company's focus by providing a trusted, hierarchical, secure, and intuitive namespace.

One of Despegar's key business segments is powering hotel reservations. The .HOTEL gTLD will become one of Despegar's core assets as it is intended to enhance Despegar's online presence and identity; expand its marketing and promotion efforts; provide a secure channel for hotel bookings and reservations; and create a marketplace for legitimate and targeted hotel- and travel-related content.

Despegar intends to initially limit registration and use of domain names within .HOTEL to Despegar and its qualified subsidiaries and affiliates. This initial limited use will allow Despegar to establish its operations and achieve full sustainability. This limited distribution, coupled with the other requirements set forth in Specification 9 of the template Registry Agreement, is intended to exempt Despegar from its annual Code of Conduct Compliance requirements.

After Stage 3 (see below), Despegar will evaluate whether opportunities exist to carry out the business strategy for the .HOTEL gTLD through expansion that continues the sustainable operations of the registry through fee-based registrations to parties other than Despegar and its qualified subsidiaries and affiliates.

Despegar currently plans a four-stage rollout for the .HOTEL gTLD:

1. Stage 1
The initial stage of implementation of the gTLD will involve Despegar registering a limited number of .HOTEL second-level domain names.

This initial use will provide Despegar's IT and security personnel the time to run a number of tests to ensure seamless and secure access using .HOTEL domain names, interoperability with various software and Web-based applications, and unbroken and secure use of all names. This initial allocation will also allow the appropriate Despegar staff to coordinate with the internal and external staff responsible for the delegation and setup phases of the .HOTEL gTLD to ensure a proper transition from delegation to full operation.

2. Stage 2
Once all testing has been successfully completed, Despegar will begin allocating domain names in .HOTEL for more widespread internal corporate use. During this same period of time, Despegar will begin evaluating strategies to potentially migrate traffic away from its current patchwork network of second-level domain names, which are registered in a variety of TLDs, to Despegar's new gTLDs.

It is in Stage 2 that Despegar will evaluate expanding the operations of the gTLD to permit registration by other registrants such as licensees and⁄or strategic partners. Should an assessment of its expansion strategy lead to a decision to extend registration rights to other parties, this expansion is currently planned to take place during Stage 3. However, any expansion would be

conditioned upon a review of Specification 9 (Registry Code of Conduct) in the template Registry Agreement to ensure compliance with Despegar's business model.

3. Stage 3
Depending on the analysis of the evaluations undertaken in Stage 2, Despegar may implement its decision to extend registration rights to licensees or strategic partners, including, but not limited to, travel companies, hotels, airlines, and other tourism organizations, depending upon compliance with Specification 9 as noted above. The dates of such expansion are subject to change depending upon business, strategic, and industry factors at the time.

After consideration of the following factors: analysis of Despegar's existing domain name portfolio; internal analysis of marketing initiatives; and the fact that Despegar will have full control over the number of registrations in the .HOTEL namespace, Despegar is confident that the number of domain name registrations will be less than 10,000 in the first five years of operation.

4. Stage 4
Based on its experience with any expansion implemented in Stage 3, Despegar will assess whether its business plan and expansion strategy should be augmented by extending registration rights to a broader class of licensees, potentially including customers of Despegar. It is anticipated by Despegar that changes to the domain name industry will take at least five years to be realized and assessed. Any decision to expand the gTLD beyond corporate, partner, and licensee use will take into account this experience as well as the technical analysis of potential expansion.

Notwithstanding the potential future expanded use of .HOTEL beginning in the sixth year of operation, Despegar currently anticipates implementing a throttle mechanism to ensure that any proposed expansion is controlled and responsible.

Specifically, under the anticipated throttle mechanism Despegar would cease registration of domain names to this potential expanded universe of registrants if and when it reaches 90 percent of the annual 50,000-domain name transaction threshold currently provided for in the template Registry Agreement. Despegar believes that is prudent to incorporate this "time-out" into the business plan in order to reevaluate potential future growth and the necessary resources to ensure that this growth does not negatively impact the secure and stable operation of the .HOTEL namespace when approaching the 50,000-domain name transaction threshold. This proposed "time-out" mechanism is described in greater detail in the responses to the financial questions (Questions 45 through 50) of this application.

The potential use of .HOTEL will also be driven by Despegar's future business strategies. Utilizing current projections based upon Despegar's existing business, future business plans, current domain name portfolio, and other strategic factors, Despegar estimates second-level domain name registrations to be in line with the projections set forth in the financial template provided in response to Question 46 of this application.

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

18.2 How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

Despegar believes that a proposed .HOTEL gTLD has the potential to offer the following benefits to Internet users and consumers:
-Establish a trusted source of information and an online marketplace for the millions of consumers who make travel reservations through Despegar's websites,

as well as serve as a secure point of sale location for numerous global hotel chains, for third parties seeking information, and for the general Internet user population searching for hotel-related content;
-Provide Despegar and its qualified subsidiaries and affiliates with short and memorable Internet addresses; provide increased navigation to products, services, advertising campaigns, public interest content, public awareness initiatives, etc.;
-Minimize the cost and need for defensive registrations because domain names within .HOTEL will only be allocated internally to Despegar and its qualified subsidiaries and affiliates, at least for the first three years of operation; and
-Develop a potential platform for secure access to, purchase of, and distribution of Despegar's services and information to its consumers in various parts of the world, in order to minimize the potential for counterfeit or infringing goods and services.

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

The primary mission and purpose of the .HOTEL gTLD is to provide a trusted, hierarchical, secure, and intuitive online marketplace to deliver Despegar's content, services, and information relating to hotels and Despegar's other offerings and information to its global customers, interested parties, and the general Internet population. As Despegar continues to expand, it wishes to pursue and develop opportunities to market and distribute its online content and products to consumers throughout Latin America, the United States, and internationally in numerous languages, and on various platforms, including the Internet and mobile devices, among others.

The tourism industry and travelers alike increasingly use the Internet as the main portal for making travel reservations. Given the increasing demand to access Despegar and its products through a variety of channels, including domain names, Despegar believes that a .HOTEL gTLD has the potential to provide an innovative, virtual avenue to Despegar goods and services that will deepen and broaden its relationship with consumers.

Most importantly, Despegar will be able to provide access to its products and online content in a targeted namespace devoid of piracy, cybersquatting, and other malicious activities. Providing consumers with a trusted experience is paramount to Despegar, and a .HOTEL gTLD will be used to further that goal by creating a safe, dedicated marketplace serving its global customer base and interested parties.

While online travel companies such as Despegar fight a never-ending battle to protect consumers from piracy on the Internet, .HOTEL would offer consumers a safe and intuitive means to access authorized content from Despegar and its qualified subsidiaries and affiliates, as well as to make reservations for travel-related services.

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

The primary driving factors of the .HOTEL gTLD are differentiation and innovation. Despegar believes that the creation of a secure and targeted space dedicated to individuals that are interested in, and businesses that offer, hotel- and travel-related content will benefit this group of consumers and businesses, as well general Internet users. The number of domain names registered will not measure the success of the gTLD, but rather success will be judged by the level of consumer recognition and trust that is placed in the .HOTEL gTLD. Using this benchmark, Despegar strives to build consumer recognition and trust through the usage of the .HOTEL gTLD that rises to the level of that found in the .EDU and .GOV gTLDs.

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

Despegar believes that the .HOTEL gTLD will provide a trusted ecosystem experience for the millions of consumers worldwide who make reservations through Despegar's sites, as well as those who seek information that Despegar provides. In addition to providing consumers with short, memorable, and intuitive domain names, the .HOTEL gTLD will indicate to consumers that all domains and content therein are owned and controlled by Despegar, thus protecting users from potential infringing, pirated, or harmful content.

The initial use of the .HOTEL gTLD will involve Despegar registering a limited number of second-level domain names. This initial use will provide Despegar's IT and security personnel the ability to run a number of tests to ensure seamless and secure access to the Despegar websites, and interoperability with various software and Web-/mobile-based applications. Once appropriate security and stability issues have been satisfactorily addressed, Despegar will likely begin allocating domain names for internal corporate use and may redirect new .HOTEL domain names to preexisting content. This phased rollout will likely take place over a multi-year period, but is subject to change depending upon a range of external factors.

During this same period of time, Despegar will evaluate potential strategies to use the .HOTEL gTLD in other ways that will advance Despegar's corporate mission and goals.

18.2.4 Provide a complete description of the applicant's intended registration policies in support of the goals listed above.

Despegar currently intends for the .HOTEL gTLD to be exclusively used by Despegar and its qualified subsidiaries and affiliates, at least for the first three years of operation. Because of this condition, Despegar intends to address registration and use requirements in its qualified subsidiary and affiliate agreements, rather than in a domain name registration agreement.

Notwithstanding this, Despegar will incorporate all required ICANN consensus policies and other legal/policy requirements imposed on new gTLD applicants into the terms and conditions of the domain name registration agreements.

18.2.5 Will your proposed gTLD impose any measures for protecting the privacy or confidential information of registrants or users? If so, please describe any such measures.

As an Internet-based travel company, Despegar recognizes that this is an evolving area of law in which there is no international standard. However, due to the fact that every domain name will be registered to Despegar and its qualified subsidiaries and affiliates, at least for the first three years of operation, Despegar has a vested interest in making sure that accurate and current domain name information is readily available in connection with each .HOTEL domain name. For the .HOTEL gTLD, all private and confidential information will be protected.

Despegar will ensure that the operation of the .HOTEL gTLD will be consistent with its privacy policy, available on its website, see http://www.us.despegar.com/commercial-web/security/confidentiality.

In addition, Despegar intends to incorporate contractual language in its Registry-Registrar Agreement (RRA) modeled after language that has been included in the template Registry Agreement and that has been successfully utilized by existing ICANN gTLD Registry Operators.

The template Registry Agreement states, "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."

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

Despegar sees the potential for this gTLD to play a large role in Despegar's future online strategic initiatives, however, there are a number of unanswered questions concerning consumer recognition, the adoption of new gTLDs, and the response from search engines in the marketplace that will influence the usage of the gTLD and communication about that usage.

Notwithstanding this, Despegar plans to start using .HOTEL domains initially as redirects to existing .COM or ccTLD domains. Despegar also plans to carefully review the release of new gTLDs by others, the response from search engines to gTLDs, and the perception of consumers. As the marketplace evolves, Despegar will invest in outreach and communication as needed to ensure that its consumers, partners, and affiliates continue to interact with Despegar content in a simplified and efficient manner.

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

18.3 What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)?

Despegar's proposed operating rules to limit registration to Despegar and its qualified subsidiaries and affiliates, at least for the first three years of operation, will provide a trusted online environment for consumers to access Despegar's online content, and by default will minimize social costs. This verified ecosystem provides consumers with a single, trusted source for Despegar goods and services with a substantially lower risk of the fraud, misdirection, infringement, or scams that consumers are plagued with in .COM and other open gTLDs. Despegar does not anticipate consumer vulnerabilities. Therefore, one way in which social costs will be eliminated is that there will be no need for other trademark and brand owners to defensively register second-level domains in the .HOTEL gTLD. In fact, Despegar's expectation is that the usage of a .HOTEL gTLD will eliminate many of the vulnerabilities that Despegar consumers face in the wider Internet today.

18.3.1 What other steps will you take to minimize negative consequences/costs imposed upon consumers?

Despegar believes that the proposed operation of the .HOTEL gTLD as set forth in this application has no known negative consequences or cost implications to consumers. On the contrary, the proposed operation of this registry will likely lead to direct and quantifiable benefits to consumers.

18.3.2 How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come/first-serve basis?

Despegar does not envision multiple applicants for the same domain name, as domain names will only be allocated to Despegar and its qualified subsidiaries and affiliates, at least for the first three years of operation, in accordance with Despegar's business plan for the .HOTEL gTLD.

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

Despegar does not envision any advantageous pricing, introductory discounts, or bulk registration discounts because these marketing/commercial initiatives are inconsistent with the mission and purpose of the .HOTEL gTLD as a trusted online source identifier. Moreover, Despegar currently intends to provide domain name registrations to itself and its qualified subsidiaries and affiliates at no cost, though the company reserves the right to reevaluate this decision and may alter it in the future.

18.3.4 Note that the Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than ten years. Additionally, the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation? If so, please describe your plans.

Despegar is committed to providing the domain name registration periods set forth in the Registry Agreement. However, as noted above, the registration and use of the domain name is conditioned upon a separate qualified subsidiary or affiliate relationship with Despegar. As such, providing contractual commitments in a domain name registrant agreement regarding the magnitude of price escalations does not seem relevant or appropriate. Additionally, as noted above, the current business model envisions Despegar providing domain name registrations to itself and its qualified subsidiaries and affiliates at no cost, at least for the first three years of operation..

Despegar acknowledges that the current template Registry Agreement requires the Registry Operator to "offer registrars the option to obtain registration periods for one to ten years at the discretion of the registrar." However, Despegar and its qualified subsidiaries and affiliates, as the sole registrants within the .HOTEL gTLD, will only be registering domain names annually. This is done to better account for annual costs, as well as to provide for more concise financial statements in Question 46 of this application; therefore there will be no multi-year registrations or deferred revenue.

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.

22.1 Despegar Online SRL has Properly Researched this Topic

Despegar Online SRL (“Despegar”) is keenly aware of the sensitivity of national governments in connection with protecting country and territory identifiers in the Domain Name System (”DNS”). In preparation for answering this question, Despegar reviewed the following relevant background material regarding the protection of geographic names in the DNS:

-ICANN Board Resolution 01-92 regarding the methodology developed for the reservation and release of country names in the .INFO top-level domain, see http:⁄⁄www.icann.org⁄en⁄minutes⁄minutes-10sep01.htm;
-ICANN’s Proposed Action Plan on .INFO Country Names, see http:⁄⁄www.icann.org⁄en⁄meetings⁄montevideo⁄action-plan-country-names-

09oct01.htm;
-"Report of the Second WIPO Internet Domain Name Process: The Recognition and Rights and the Use of Names in the Internet Domain Name System," Section 6, Geographical Identifiers, see http://www.wipo.int/amc/en/processes/process2/report/html/report.html;
- ICANN's Governmental Advisory Committee (GAC) Principles Regarding New gTLDs, see https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000; and
-ICANN's Generic Names Supporting Organization Reserved Names Working Group – Final Report, see http://gnso.icann.org/issues/new-gtlds/final-report-rn-wg-23may07.htm.

22.2 Initial Reservation of Country and Territory Names

Despegar is committed to initially reserving the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 attached to the Applicant Guidebook at the second level and at all other levels within the .HOTEL gTLD at which Despegar will provide registrations. Specifically, Despegar will reserve:

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, see 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; and

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

22.3 Fair & Non-Misleading Use of Geographical Identifiers

Despegar is part of the largest online travel agency in all of Latin America and is a leading multinational tourism organization that enables customers to book airline tickets, hotel rooms, rental cars, vacation packages, and other travel-related services, and also powers travel bookings for various airlines, hotels, rental car agencies, and other tourism-related organizations internationally. Despegar serves more than five million clients annually and has a presence in 21 countries. Its services and online content are accessible in the .COM gTLD and the .AR, .BO, .BR, .CC, .CL, .CO, .CR, .DO, .EC, .ES, .HN, .MX, .PA, .PE, .PR, .PY, .TV, .US, .UY, .VE, and .WS ccTLDs.

Despegar is applying for five generic-term gTLDs: .VUELOS and .HOTELES, which target Despegar's Spanish-speaking customers and Internet users; .PASSAGENS and .HOTEIS, which target Despegar's Portuguese-speaking customers and Internet users; and .HOTEL, which targets Despegar's English, Spanish, and Portuguese-speaking customers and Internet users.

In providing online content, sales, and services to customers throughout the world, Despegar makes regular use of geographical identifiers to provide consumers with a hierarchical and intuitive namespace to navigate for relevant content. For example, on its home page, users have the ability to select a country in order to receive the appropriate, geographically specific content, see www.Despegar.com.

Despegar would like to provide a hierarchical and intuitive framework for the .HOTEL namespace by using geographical identifiers as second-level domain

names. This use of geographical identifiers to the left of the gTLD and as part of the domain name itself is believed to have a direct and material impact on search engine algorithms and their corresponding query results. Despegar would like to see if this type of hierarchical and intuitive use of second-level domain names within a gTLD provides increased consumer functionality and innovation, as premised by ICANN.

Currently, Despegar operates a number of corporate websites using a combination of second-level and top-level domain names. A representative sampling of Despegar websites that incorporate geographical identifiers into the domain name include:

Despegar.cl
Despegar.com.bo
Despegar.com.ve
DespegarPeru.com

Despegar believes that a .HOTEL gTLD can provide an online, single-source identifying function for its current and future customers around the world who are seeking to make hotel reservations and other travel-related arrangements. This is in contrast to the present approach Despegar has used as it expands into different markets around the world, which consists of registering the domain names that are available, rather than those that may be the most intuitive.

22.4 The Legal Protection of Geographical Identifiers

One of the more authoritative resources on the current state of the law in connection with the protection of geographical identifiers was authored by the World Intellectual Property Organization (WIPO) in its 2001 "Report of the Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System" publication. Section six of this report was devoted exclusively to the protection of geographical identifiers.

In analyzing the well-established framework against the misuse of geographical identifiers at the international, regional, and national levels, WIPO identified the following two elements for the protection of geographical identifiers: (i) a prohibition of false descriptions of the geographical source of goods; and (ii) a more extensive set of rules prohibiting the misuse of one class of geographical source indicators, known as geographical indications (see "Report of the Second WIPO Internet Domain Name Process," Paragraphs 206 and 210). Neither false descriptions of the geographical source of goods, nor misuse of geographical indications, is present in Despegar's current or proposed use of geographical identifiers.

Notwithstanding WIPO's recommendation that the protection of geographical identifiers is "a difficult area on which views are not only divided, but also ardently held" (Paragraph 237) national governments within the ICANN Governmental Advisory Committee (GAC) and other international forums have continued to advocate for increased safeguards to protect against the misuse of geographical identifiers within the domain name system.

Despegar, acting as a responsible international business, seeks to minimize any potential business practices that might mislead consumers. However, at the same time, it believes that it is important to be able to use geographical identifiers in a fair use and non-misleading manner, if such use can benefit Internet users as proposed in Despegar's business model.

22.5 Samples of Fair & Non-Misleading Use of Geographical Identifiers

In undertaking a thorough research of this subject matter prior to filing this application, Despegar's subject matter experts were able to uncover the following representative sampling of fair and non-misleading use of geographical identifiers used in the existing gTLD domain name space:

Fair Use of National Geographical Identifiers

AUSTRALIA.COOP – Is operated by Co-operatives Australia, the national body for State Co-operative Federations, and provides a valuable resource about cooperatives within Australia.

USA.JOBS – Is operated by DirectEmployers Association ("DE"). While Employ Media, the registry operator of the .JOBS gTLD, is currently in a dispute with ICANN regarding the allocation of this and other domain names, DE has a series of partnerships and programs with the United States Department of Labor, the National Association of State Workforce Agencies, and Facebook to help unemployed workers find jobs.

MALDIVIAN.AERO – Is the dominant domestic air carrier in Maldives, and provides a range of commercial and leisure air transport services.

Fair Use of Regional⁄Local Geographical Indicators

BROOKLYN.COOP – Is operated by Brooklyn Cooperative Federal Credit Union, which began as a modest storefront business in 2001, but is now New York City's fastest growing credit union and a model for community development credit unions nationwide.

HYDERABAD.AERO – Is operated by the Hyderabad International Airport and provides a range of interactive services and information for both business and leisure travelers.

SACRAMENTO.AERO – Is a portal website operated by Sacramento County to provide links to each of the airports serving the Sacramento area: Sacramento International Airport (SMF), Mather Airport (MHR), Executive Airport (SAC), and Franklin Field (F72).

22.6 Protection of Regional and Local Geographic Names for Non-Misleading Use

Despegar has stated its intention to consider using non-reserved geographic identifiers as part of a hierarchical and intuitive framework in a fair and non-misleading manner to help consumers navigate the .HOTEL namespace. Despegar is committed to operating the .HOTEL namespace in a manner that minimizes potential consumer confusion, and will actively work with others in the ICANN community regarding any future policy development in this area.

22.7 Potential Future Release of Initially Reserved Names

Given that Despegar is an international organization currently operating in numerous countries, Despegar looks forward to collaborating with other new gTLD registry operators in potentially working with ICANN's GAC to explore potential processes that could permit the release of initially reserved country names (including ISO-3166 two-characters). Specifically, Despegar is interested in exploring other Registry Service Evaluation Processes (RSEP) that have been filed by existing gTLD registry operators in releasing previously reserved domain names.

22.8 Dispute Resolution

Despegar does not envision any potential disputes from governments or public authorities in connection with the registration and use of geographic names within the .HOTEL gTLD based upon its proposed use, set forth in the response to Question 18 of this application.

However, Despegar is committed to working with governments, public authorities, or IGOs that may have a concern regarding the registration of names with national or geographic significance at the second level within .HOTEL. Therefore, should there arise any potential disputes, Despegar will undertake

an immediate policy development process as identified below.

22.9 Creation and Updating the Policies

If there should arise some future need for the creation or updating of the policies regarding this class of domain names, Despegar will act in an open and transparent manner consistent with its prior practices to develop such a policy and/or recommendation.

Despegar is also committed to continually reviewing and updating these lists to prevent the misleading use of geographical identifiers. Consistent with this commitment, Despegar intends to remain an active participant in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS.

Registry Services

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

23.1 Introduction
Despegar Online SRL ("Despegar") has elected to partner with Neustar, Inc. ("Neustar") to provide back-end services for the .HOTEL registry. In making this decision, Despegar recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .HOTEL registry. The following section describes the registry services to be provided.
23.2 Standard Technical and Business Components
Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. Despegar will use Neustar's Registry Services platform to deploy the .HOTEL registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .HOTEL:
Registry-Registrar Shared Registration Service (SRS)
Extensible Provisioning Protocol (EPP)
Domain Name System (DNS)
WHOIS
DNSSEC
Data Escrow
Dissemination of Zone Files using Dynamic Updates
Access to Bulk Zone Files
Dynamic WHOIS Updates
IPv6 Support
Rights Protection Mechanisms
Internationalized Domain Names (IDN)
The following is a description of each of the services:
SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.
EPP
The .HOTEL registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP

based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.

DNS

Despegar will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.

WHOIS

Neustar's existing standard WHOIS solution will be used for the .HOTEL. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy and is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:

Standard WHOIS (Port 43)

Standard WHOIS (Web)

Searchable WHOIS (Web)

DNSSEC

An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .BIZ, .US, and .CO. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question 43.

Data Escrow

Data Escrow will be performed in compliance with all ICANN requirements in conjunction with an approved Data Escrow provider. The Data Escrow service will:

Protect against data loss

Follow industry best practices

Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure

Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.

Dissemination of Zone Files using Dynamic Updates

Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.

Access to Bulk Zone Files

Despegar will provide third-party access to the bulk zone file in accordance with Specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.

Dynamic WHOIS Updates

Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

IPv6 Support

The .HOTEL registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS⁄DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.

Required Rights Protection Mechanisms

Despegar will provide all ICANN required Rights Mechanisms, including:

Trademark Claims Service
Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
Registration Restriction Dispute Resolution Procedure (RRDRP)
UDRP
URS
Sunrise service
More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)
IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.
23.3 Unique Services
The only unique service that Despegar is considering at this time is the potential imposition of an annual cost recovery based fee to validate registrars that will be providing domain name registration services in the .HOTEL gTLD.

An additional service which Despegar may offer, commonly used in the marketplace today, is the use of RFPs (Request for Proposals) and Auctions to determine string allocation in appropriate circumstances.
23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

24.1 Introduction
Despegar Online SRL (“Despegar”) has partnered with Neustar, Inc. (“Neustar”) an experienced TLD Registry Operator, for the operation of the .HOTEL registry. Despegar is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.
Neustar built its SRS from the ground up as an EPP-based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO, and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar’s state-of-the-art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.
The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.
24.2 The Plan for Operation of a Robust and Reliable SRS
High-level SRS System Description
The SRS to be used for .HOTEL will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the New gTLD Applicant Guidebook.
The SRS is the central component of any registry implementation and its quality, reliability, and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations

with proven and verifiable performance, reliability, and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, Despegar is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:
State-of-the-art, production-proven, multi-layer design;
Ability to rapidly and easily scale from low to high volume as a TLD grows;
Fully redundant architecture at two sites;
Support for IDN registrations in compliance with all standards;
Use by over 300 Registrars;
EPP connectivity over IPv6;
Performance being measured using 100% of all production transactions (not sampling); and
SRS Systems, Software, Hardware, and Interoperability.
The systems and software that the registry operates on are a critical element to providing a high quality of service. If the systems are of poor quality, if they are difficult to maintain and operate, or if the registry personnel are unfamiliar with them, the registry will be prone to outages. Neustar has a decade of experience operating registry infrastructure to extremely high service level requirements. The infrastructure is designed using best of breed systems and software. Much of the application software that performs registry-specific operations was developed by the current engineering team and as a result, the team is intimately familiar with its operations.
The architecture is highly scalable and provides the same high level of availability and performance as volumes increase. It combines load-balancing technology with scalable server technology to provide a cost effective and efficient method for scaling.
The registry is able to limit the ability of any one registrar from adversely impacting other registrars by consuming too many resources due to excessive EPP transactions. The system uses network layer 2 level packet shaping to limit the number of simultaneous connections registrars can open to the protocol layer.
All interaction with the registry is recorded in log files. Log files are generated at each layer of the system. These log files record at a minimum:
The IP address of the client;
Timestamp;
Transaction Details; and
Processing Time.
In addition to logging of each and every transaction with the SRS, Neustar maintains audit records, in the database, of all transformational transactions. These audit records allow the registry, in support of Despegar, to produce a complete history of changes for any domain name.
SRS Design
The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:
Protocol Layer;
Business Policy Layer; and
Database.
Each of the layers is described below.
Protocol Layer
The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.
The EPP servers authenticate against a series of security controls before granting service, as follows:
The registrar’s host exchanges keys to initiates a TLS handshake session with the EPP server.
The registrar’s host must provide credentials to determine proper access levels.
The registrar’s IP address must be preregistered in the network firewalls and traffic-shapers.
Business Policy Layer
The Business Policy Layer is the “brain” of the registry system. Within this

layer, the policy engine servers perform rules-based processing as defined through configurable attributes. This process takes individual transactions, applies various validation and policy rules, persists data, and dispatches notification through the central database in order to publish to various external systems. External systems fed by the Business Policy Layer include back-end processes such as dynamic update of DNS, WHOIS, and Billing.
Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes.
The SRS today processes over 30 million EPP transactions daily.
Database
The database is the third core component of the SRS. The primary function of the SRS database is to provide highly reliable, persistent storage for all registry information required for domain registration services. The database is highly secure, with access limited to transactions from authenticated registrars, trusted application-server processes, and highly restricted access by the registry database administrators. A full description of the database can be found in response to Question 33.
See attachment: Figure 24-1, which depicts the overall SRS architecture including network components. This multi-layer architecture is EPP-compliant, meets all applicable RFCs, and its development follows industry best-practices.
Number of Servers
As depicted in the SRS architecture diagram above, Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs, as do the databases. For the .HOTEL registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth.
In addition to the SRS servers described above, there are multiple back-end servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.
Description of Interconnectivity with Other Registry Systems
The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:
WHOIS;
DNS;
Billing; and
Data Warehouse (Reporting and Data Escrow).
Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for .HOTEL.
The SRS includes an "External Notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming back-end processing to be decoupled from critical online registrar transactions. Using an External Notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back-end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three External Notifiers used the SRS:
WHOIS External Notifier
The WHOIS External Notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS External Notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS External Notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence

and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.

DNS External Notifier

The DNS External Notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS External Notifier, the DNS External Notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.

Billing External Notifier

The Billing External Notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This External Notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse

The Data Warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of Data Escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The Data Warehouse databases are updated on a daily basis with full copies of the production SRS data.

Frequency of Synchronization between Servers

The External Notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.

Synchronization Scheme (e.g., hot standby, cold standby)

Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated in real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.

Compliance with Specification 6 Section 1.2

The SRS implementation for .HOTEL is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and Registry-Registrar Agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

See attachment: Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.

Compliance with Specification 10

Specification 10 of the New TLD Registry Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced Registry Operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .HOTEL registry. The following section describes Neustar’s experience and its capabilities to meet the requirements in the new agreement.

To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar’s current .BIZ SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

See attachment: Table 24-2.
Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.
24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:
Development/Engineering;
Database Administration;
Systems Administration; and
Network Engineering.
Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.
The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .HOTEL registry. The following resources are available from those teams:
Development/Engineering – 19 employees
Database Administration – 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees
The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .HOTEL registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction
Despegar Online SRL ("Despegar") back-end registry operator, Neustar, Inc. ("Neustar") has over 10 years of experience operating EPP-based registries. They deployed one of the first EPP registries in 2001 with the launch of .BIZ. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure Despegar is provided with an unparalleled EPP-based registry. The following discussion explains the EPP interface, which will be used for the .HOTEL registry. This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.
See attachment: Figure 25-1. The protocol layer is responsible for ensuring transactions comply with the appropriate protocol.
25.2 EPP Interface
Registrars are provided with two different interfaces for interacting with the registry. Both are EPP-based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry.
However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:
Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.

Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
Extensibility: The software is built ground-up using object-oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
Security: The system provides IP address-based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.
25.3 Compliance with RFCs and Specifications
The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.
See attachment: Table 25-1.
Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.
Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar's ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.
See attachment: Table 25-2.
EPP Toolkits
Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.
The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a "dummy" server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.
25.3 Proprietary EPP Extensions
The .HOTEL registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other

TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the .HOTEL registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.
See attachment: Table 25-3.
The full EPP schema to be used in the .HOTEL registry is attached in the document titled "EPP Schema."
25.4 Resourcing Plans
The development and support of EPP is largely the responsibility of the Development/Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Quality Assurance – 7 employees.
These resources are more than adequate to support any EPP modification needs of the .HOTEL registry.

26. Whois

26.1 Introduction
Despegar Online SRL ("Despegar") recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders, and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 of the Registry Agreement. Despegar's back-end registry services provider, Neustar, Inc. ("Neustar"), has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs and ccTLDs, and as a back-end registry services provider. As one of the first "thick" Registry Operators in the gTLD space, Neustar's WHOIS service has been designed from the ground up to display as much information as required by a TLD and to respond to a very stringent availability and performance requirement.
Some of the key features of .HOTEL's solution include:
Fully compliant with all relevant RFCs including 3912;
Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years;
Exceeds current and proposed performance specifications;
Supports dynamic updates with the capability of doing bulk updates; and
Geographically distributed sites to provide greater stability and performance.
In addition, .HOTEL's thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).
26.2 Software Components
The WHOIS architecture comprises the following components:
An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.
Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.
Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be

readily applied.
Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.
Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.
Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.
Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization.
SRS master database: The SRS database is the main persistent store of the registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.
26.3 Compliance with RFC and Specifications 4 and 10
Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. RFC 3912 is a simple text-based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.
See attachment: Table 26-1, which describes Neustar's compliance with Specifications 4 and 10.
Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.
26.4 High-level WHOIS System Description
26.4.1 WHOIS Service (port 43)
The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves.
The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name's UTF-8 encoded representation along with the Unicode code page.
26.4.2 Web Page for WHOIS queries
In addition to the WHOIS Service on port 43, Neustar provides a Web-based WHOIS application (www.whois.tld). It is an intuitive and easy to use application for the general public to use. The WHOIS Web-application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:
Domain names;
Nameservers;
Registrant, Technical, and Administrative Contacts; and
Registrars.
It also provides features not available on the port 43 service. These include:
Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the Web-based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
Extensive support for international domain names (IDN);
Ability to perform WHOIS lookups on the actual Unicode IDN;
Display of the actual Unicode IDN in addition to the ACE-encoded name;
A Unicode to Punycode and Punycode to Unicode translator;
An extensive FAQ; and
A list of upcoming domain deletions.

26.5 IT and Infrastructure Resources
As described above, the WHOIS architecture uses a workflow that decouples the update process from the SRS. This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:
Firewalls, to protect this sensitive data;
Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates;
Packetshaper for source IP address-based bandwidth limiting;
Load balancers to distribute query load; and
Multiple WHOIS servers for maximizing the performance of WHOIS service.
The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
See attachment: Figure 26-1, which depicts the different components of the WHOIS architecture. WHOIS is decoupled from the architecture to protect production databases and increased overall systems security.
26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, "Technical Overview," when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer. The update agent processes these updates, transforms the data if necessary and then uses messaging-oriented middleware to publish all updates to each WHOIS slave. The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.
26.7 Frequency of Synchronization between Servers
Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish⁄subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% ≤ 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% ≤ 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.
26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new Web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will enable users to search the WHOIS directory using any one or more of the following fields:
Domain name;
Registrar ID;
Contact's and registrant's name;
Contact's and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.); and
Name server name and name server IP address
The system will also allow search using non-Latin character sets, which are compliant with IDNA specification.
The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
See attachment: Figure 26-2, which shows an architectural depiction of the new service. Neustar's Web-based service provides new search features based on requirements specified in Specification 4 Section 1.8.
To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine, which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:
Data Mining;
Unauthorized Access;
Excessive Querying; and
Denial of Service Attacks.

To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:
Username-password based authentication;
Certificate based authentication;
Data encryption;
CAPTCHA mechanism to prevent robo invocation of Web query; and
Fee-based advanced query capabilities for premium customers.
The searchable WHOIS application will adhere to all privacy laws and policies of the .HOTEL registry.
26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:
Development⁄Engineering – 19 employees
Database Administration – 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees
Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the .HOTEL registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .HOTEL registry.

27. Registration Life Cycle

27.1 Registration Life Cycle
Introduction
Despegar Online SRL ("Despegar") will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be use for .HOTEL.
Domain Lifecycle - Description
The registry will use the EPP 1.0 standard for provisioning domain names, contacts, and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts.
Domains, contacts, and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the .HOTEL registry per the defined .HOTEL business rules.
The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.
OK – Default status applied by the Registry.
Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.
PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the .HOTEL registry.

PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.
PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.
PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the .HOTEL registry.
PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in the .HOTEL registry.
Hold – Removes the domain from the DNS zone.
UpdateProhibited – Prevents the object from being modified by an Update command.
TransferProhibited – Prevents the object from being transferred to another Registrar by the Transfer command.
RenewProhibited – Prevents a domain from being renewed by a Renew command.
DeleteProhibited – Prevents the object from being deleted by a Delete command.
The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above. Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:
Domain may be updated
Domain may be deleted, either within or after the add-grace period
Domain may be renewed at anytime during the term
Domain may be auto-renewed by the Registry
Domain may be transferred to another registrar.
Each of these actions may result in a change in domain state. This is described in more detail in the following section. Every domain must eventually be renewed, auto-renewed, transferred, or deleted. A registrar may apply EPP statuses described above to prevent specific actions such as updates, renewals, transfers, or deletions.
27.1.1 Registration States
Domain Lifecycle – Registration States
As described above, the .HOTEL registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:
Active
Inactive
Locked
Pending Transfer
Pending Delete
All domains are always in either an Active or Inactive state, and throughout the course of the lifecycle may also be in a Locked, Pending Transfer, and Pending Delete state. Specific conditions such as applied EPP policies and registry business rules will determine whether a domain can be transitioned between states. Additionally, within each state, domains may be subject to various timed events such as grace periods, and notification periods.
Active State
The active state is the normal state of a domain and indicates that delegation data has been provided and the delegation information is published in the zone. A domain in an Active state may also be in the Locked or Pending Transfer states.
Inactive State
The Inactive state indicates that a domain has not been delegated or that the delegation data has not been published to the zone. A domain in an Inactive state may also be in the Locked or Pending Transfer states. By default all domain in the Pending Delete state are also in the Inactive state.
Locked State

The Locked state indicates that certain specified EPP transactions may not be performed to the domain. A domain is considered to be in a Locked state if at least one restriction has been placed on the domain; however up to eight restrictions may be applied simultaneously. Domains in the Locked state will also be in the Active or Inactive, and under certain conditions may also be in the Pending Transfer or Pending Delete states.

Pending Transfer State

The Pending Transfer state indicates a condition in which there has been a request to transfer the domain from one registrar to another. The domain is placed in the Pending Transfer state for a period of time to allow the current (losing) registrar to approve (ack) or reject (nack) the transfer request. Registrars may only nack requests for reasons specified in the Inter-Registrar Transfer Policy.

Pending Delete State

The Pending Delete State occurs when a Delete command has been sent to the Registry after the first 5 days (120 hours) of registration. The Pending Delete period is 35-days during which the first 30-days the name enters the Redemption Grace Period (RGP) and the last 5-days guarantee that the domain will be purged from the Registry Database and available to public pool for registration on a first come, first serve basis.

27.1.2 Typical Registration Lifecycle Activities

Domain Creation Process

The creation (registration) of domain names is the fundamental registry operation. All other operations are designed to support or complement a domain creation. The following steps occur when a domain is created.

Contact objects are created in the SRS database. The same contact object may be used for each contact type, or they may all be different. If the contacts already exist in the database this step may be skipped.

Nameservers are created in the SRS database. Nameservers are not required to complete the registration process; however any domain with less than 2 name servers will not be resolvable.

The domain is created using the each of the objects created in the previous steps. In addition, the term and any client statuses may be assigned at the time of creation.

The actual number of EPP transactions needed to complete the registration of a domain name can be as few as one and as many as 40. The latter assumes seven distinct contacts and 13 nameservers, with Check and Create commands submitted for each object.

Update Process

Registry objects may be updated (modified) using the EPP Modify operation. The Update transaction updates the attributes of the object.

For example, the Update operation on a domain name will only allow the following attributes to be updated:

Domain statuses
Registrant ID
Administrative Contact ID
Billing Contact ID
Technical Contact ID
Nameservers
AuthInfo
Additional Registrar provided fields

The Update operation will not modify the details of the contacts. Rather it may be used to associate a different contact object (using the Contact ID) to the domain name. To update the details of the contact object the Update transaction must be applied to the contact itself. For example, if an existing registrant wished to update the postal address, the Registrar would use the Update command to modify the contact object, and not the domain object.

Renew Process

The term of a domain may be extended using the EPP Renew operation. ICANN policy general establishes the maximum term of a domain name to be 10 years, and Neustar recommends not deviating from this policy. A domain may be renewed/extended at any point time, even immediately following the initial registration. The only stipulation is that the overall term of the domain name may not exceed 10 years. If a Renew operation is performed with a term value

will extend the domain beyond the 10-year limit, the Registry will reject the transaction entirely.
Transfer Process
The EPP Transfer command is used for several domain transfer related operations:
Initiate a domain transfer
Cancel a domain transfer
Approve a domain transfer
Reject a domain transfer
To transfer a domain from one Registrar to another the following process is followed:
The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into PendingTransfer status
A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar's message queue
The domain remains in PendingTransfer status for up to 120 hours, or until the losing (current) Registrar Acks (approves) or Nack (rejects) the transfer request
If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer
The requesting Registrar may cancel the original request up until the transfer has been completed.
A transfer adds an additional year to the term of the domain. In the event that a transfer will cause the domain to exceed the 10-year maximum term, the Registry will add a partial term up to the 10 year limit. Unlike with the Renew operation, the Registry will not reject a transfer operation.
Deletion Process
A domain may be deleted from the SRS using the EPP Delete operation. The Delete operation will result in either the domain being immediately removed from the database or the domain being placed in PendingDelete status. The outcome is dependent on when the domain is deleted. If the domain is deleted within the first five days (120 hours) of registration, the domain is immediately removed from the database. A deletion at any other time will result in the domain being placed in PendingDelete status and entering the Redemption Grace Period (RGP). Additionally, domains that are deleted within five days (120) hours of any billable (add, renew, transfer) transaction may be deleted for credit.
27.1.3 Applicable Time Elements
The following section explains the time elements that are involved
Grace Periods
There are six grace periods:
Add-Delete Grace Period (AGP)
Renew-Delete Grace Period
Transfer-Delete Grace Period
Auto-Renew-Delete Grace Period
Auto-Renew Grace Period
Redemption Grace Period (RGP).
The first four grace periods listed above are designed to provide the Registrar with the ability to cancel a revenue transaction (add, renew, or transfer) within a certain period of time and receive a credit for the original transaction.
The following describes each of these grace periods in detail.
Add-Delete Grace Period
The APG is associated with the date the Domain was registered. Domains may be deleted for credit during the initial 120 hours of a registration, and the Registrar will receive a billing credit for the original registration. If the domain is deleted during the Add Grace Period, the domain is dropped from the database immediately and a credit is applied to the Registrar's billing account.
Renew-Delete Grace Period
The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may be deleted for credit during the 120 hours after a renewal. The grace period is intended to allow Registrars to correct domains

that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into PendingDelete and will enter the RGP (see below).
Transfer-Delete Grace Period
The Transfer-Delete Grace Period is associated with the date the Domain was transferred to another Registrar. Domains may be deleted for credit during the 120 hours after a transfer. It should be noted that domains that are deleted during the renew grace period will be placed into PendingDelete and will enter the RGP. A deletion of domain after a transfer is not the method used to correct a transfer mistake. Domains that have been erroneously transferred or hijacked by another party can be transferred back to the original registrar through various means including contacting the Registry.
Auto-Renew-Delete Grace Period
The Auto-Renew-Delete Grace Period is associated with the date the Domain was auto-renewed. Domains may be deleted for credit during the 120 hours after an auto-renewal. The grace period is intended to allow Registrars to correct domains that were mistakenly auto-renewed. It should be noted that domains that are deleted during the auto-renew delete grace period will be placed into PendingDelete and will enter the RGP.
Auto-Renew Grace Period
The Auto-Renew Grace Period is a special grace period intended to provide registrants with an extra amount of time, beyond the expiration date, to renew their domain name. The grace period lasts for 45 days from the expiration date of the domain name. Registrars are not required to provide registrants with the full 45 days of the period.
Redemption Grace Period
The RGP is a special grace period that enables Registrars to restore domains that have been inadvertently deleted but are still in PendingDelete status within the Redemption Grace Period. All domains enter the RGP except those deleted during the AGP.
The RGP period is 30 days, during which time the domain may be restored using the EPP RenewDomain command as described below. Following the 30day RGP period the domain will remain in PendingDelete status for an additional five days, during which time the domain may NOT be restored. The domain is released from the SRS, at the end of the 5-day non-restore period. A restore fee applies and is detailed in the Billing Section. A renewal fee will be automatically applied for any domain past expiration.
Neustar has created a unique restoration process that uses the EPP Renew transaction to restore the domain and fulfill all the reporting obligations required under ICANN policy. The following describes the restoration process.
27.2 State Diagram
See attachment: Figure 27-1, which provides a description of the registration lifecycle.
The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.
The details of each trigger are described below:
Create: Registry receives a create domain EPP command.
WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
WithOutNS: The domain has not met the minimum number of nameservers required by registry policy. The domain will not be in the DNS zone.
Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
Delete: Registry receives a delete domain EPP command.
DeleteAfterGrace: Domain deletion does not fall within the add grace period.
DeleteWithinAddGrace: Domain deletion falls within add grace period.

Restore: Domain is restored. Domain goes back to its original state prior to the delete command.
Transfer: Transfer request EPP command is received.
Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.
TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.
DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status. This will cause the delete command to fail. The domain goes back to its original state.
Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.
27.2.1 EPP RFC Consistency
As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.
27.3 Resources
The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working with Despegar to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team. Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The .HOTEL registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Registry Product Management – 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the .HOTEL registry.

28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation
Strong abuse prevention of a new gTLD is an important benefit to the Internet community. Despegar Online SRL ("Despegar") and its back-end registry services provider, Neustar, Inc. ("Neustar"), agree that a registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the public interest. Neustar brings extensive experience establishing and implementing registration policies. This experience will be leveraged to help Despegar combat abusive and malicious domain activity within the new gTLD space.
One of those public interest functions for a responsible domain name registry includes working towards the eradication of abusive domain name registrations, including, but not limited to, those resulting from:
Illegal or fraudulent actions
Spam
Phishing
Pharming
Distribution of malware
Fast flux hosting
Botnets
Distribution of child pornography

Online sale or distribution of illegal pharmaceuticals
More specifically, although traditionally botnets have used Internet Relay Chat (IRC) servers to control registry and the compromised PCs, or bots, for DDoS attacks and the theft of personal information, an increasingly popular technique, known as fast-flux DNS, allows botnets to use a multitude of servers to hide a key host or to create a highly-available control network. This ability to shift the attacker's infrastructure over a multitude of servers in various countries creates an obstacle for law enforcement and security researchers to mitigate the effects of these botnets. But a point of weakness in this scheme is its dependence on DNS for its translation services. By taking an active role in researching and monitoring these sorts of botnets, Despegar's partner, Neustar, has developed the ability to efficiently work with various law enforcement and security communities to begin a new phase of mitigation of these types of threats.
Policies and Procedures to Minimize Abusive Registrations
A registry must have the policies, resources, personnel, and expertise in place to combat such abusive DNS practices. As Despegar's registry provider, Neustar is at the forefront of the prevention of such abusive practices and is one of the few registry operators to have actually developed and implemented an active "domain takedown" policy. We also believe that a strong program is essential given that registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet, often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name registrant, but also to millions of unsuspecting Internet users.
Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. Despegar has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.
Abuse Point of Contact
As required by the Registry Agreement, Despegar will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. Despegar will also provide such information to ICANN prior to the delegation of any domain names in the TLD. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. We will ensure that this information will be kept accurate and up-to-date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited registrars, our registry services provider, Neustar, shall have an additional point of contact, as it does today, handling requests by registrars related to abusive domain name practices.
28.2 Policies Regarding Abuse Complaints
One of the key policies each new gTLD registry will need to have is an Acceptable Use Policy that clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. In addition, the policy will be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the registry to take the appropriate actions based on the type of abuse. This will include locking down the domain name, preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name "on hold," rendering the domain name non-resolvable, transferring to the domain name to another registrar, and⁄or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation.
Despegar will adopt an Acceptable Use Policy that clearly defines the types of activities that will not be permitted in the TLD and reserves the right to

lock, cancel, transfer, or otherwise suspend or take down domain names violating the Acceptable Use Policy and allow the registry where and when appropriate to share information with law enforcement. Each ICANN-Accredited Registrar must agree to pass through the Acceptable Use Policy to its Resellers (if applicable) and ultimately to the TLD registrants. Below is the registry's initial Acceptable Use Policy that we will use in connection with the .HOTEL TLD.

.HOTEL Acceptable Use Policy

This Acceptable Use Policy gives the registry the ability to quickly lock, cancel, transfer, or take ownership of any .HOTEL domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity, or security of the registry, or any of its registrar partners – and⁄or that may put the safety and security of any registrant or user at risk. The process also allows the registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the ongoing monitoring by the registry or its partners. In all cases, the registry or its designees will alert registry's registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than .HOTEL's own.

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

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

Fast Flux Hosting: a technique used to shelter Phishing, Pharming, and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.

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

Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.

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

The registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the registry reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by the registry or any registrar in connection with a domain name registration. The registry also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and⁄or Malicious Activity

The registry is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the TLD, or are part of a real-time investigation by law enforcement.

Once a complaint is received from a trusted source, third party, or detected by the registry, the registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the registry, the sponsoring registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the registry will place the domain on "ServerHold." Although this action removes the domain name from the TLD zone, the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Coordination with Law Enforcement

With the assistance of Neustar as its back-end registry services provider, Despegar can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. The registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by Despegar for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by the registry and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar is then given 12 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the registry will place the domain on "serverHold."

28.2 Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (SSAC) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the "dominant use of orphaned glue supports the correct and ordinary operation of the DNS." See http://www.icann.org/en/committees/security/sac048.pdf.

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

Neustar runs a daily audit of entries in its DNS systems and compares those with its provisioning system. This serves as an umbrella protection to make sure that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system will be flagged for investigation and removed if necessary. This daily DNS audit serves to not only prevent orphaned hosts but also other records that should not be in the zone.

In addition, if either Despegar or Neustar becomes aware of actual abuse on orphaned glue after receiving written notification by a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.3 Measures to Promote WHOIS Accuracy

Despegar acknowledges that ICANN has developed a number of mechanisms over the

past decade that are intended to address the issue of inaccurate WHOIS information.
However, the proposed use of .HOTEL as a gTLD in which all of the domain names will initially be registered by Despegar and its qualified subsidiaries and affiliates essentially eliminates the potential of false or inaccurate WHOIS data. Further ensuring that all domain names contain uniform, accurate, and up-to-date WHOIS information is the fact that these domain names will be registered through Despegar's existing registrar(s), or a similarly situated registrar, which handle Despegar's existing domain name portfolio.
Should Despegar expand the universe of potential registrants in the .HOTEL namespace, to include third parties such as licensees or strategic partners, Despegar intends to offer the following enhanced mechanism to ensure the accuracy of WHOIS data, specifically, a mechanism whereby third parties can submit complaints directly to Despegar (as opposed to ICANN or the sponsoring registrar) about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, Despegar will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the registrar has failed to take any action, or it is clear that the registrant was either unwilling or unable to correct the inaccuracies, Despegar reserves the right to suspend the applicable domain name(s) until such time as the registrant is able to cure the deficiencies.
In addition, should Despegar expand the universe of potential registrants within the .HOTEL namespace to include third parties such as licensees or strategic partners, Despegar shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of .HOTEL domain names to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, Despegar will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring registrar, who shall be required to address those complaints with its registrants. Thirty days after forwarding the complaint to the registrar, the Despegar will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the registrar has failed to take any action, or it is clear that the registrant was either unwilling or unable to correct the inaccuracies, Despegar reserves the right to suspend the applicable domain name(s) until such time as the registrant is able to cure the deficiencies.
28.3.1 Authentication of Registrant Information
As noted above, the proposed use of the .HOTEL as a .BRAND gTLD in which all domain names will initially be registered by Despegar to Despegar, or its qualified subsidiaries and affiliates, essentially eliminates the potential of false or inaccurate WHOIS data. Additionally, all domain names will be registered through Despegar's corporate registrar, or a similar corporate registrar, which employs enhanced security protocols that limit which employees can register domain names, as well as ensure that those domain names that are registered contain uniform, accurate, and up-to-date WHOIS information.
Should Despegar expand the universe of potential registrants within the .HOTEL namespace to include third parties such as licensees or strategic partners, such domain names would not be permitted to be registered until Despegar had a process in place to verify the identity of the registrant and the accuracy of the WHOIS data.
28.3.2 Monitoring of Registration Data
As noted above Despegar will provide a mechanism by which third parties can submit a WHOIS accuracy complaint directly to the Registry Operator for timely investigation and resolution. In addition, Despegar has committed to perform a manual review of a random sampling of .HOTEL domain names no less than twice per year to test the accuracy of the WHOIS information after the expanding the potential universe of domain names to include third parties such as licensees or strategic partners.
28.3.3 Policies and Procedures Ensuring Compliance

These proposed enhanced safeguards designed to promote the accuracy of WHOIS data will be hard coded into the Registry-Registrar Agreement (RRA) as well as the end-registrant agreement. Despegar will proactively be monitoring similar gTLDs to ensure best in class policies to promote the accuracy and availability of WHOIS data.

28.4 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups. The Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The customer service team also plays an important role in assisting with the investigations, responded to customers, and notifying registrars of abusive domains. Finally, the Policy⁄Legal team is responsible for developing the relevant policies and procedures.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:

Customer Support – 12 employees

Policy⁄Legal – 2 employees

In addition to the above staffing provided by Neustar, Despegar will provide the full support of its internal staff (2.0 FTE count) as well as its external vendors where the situation requires the extra staffing resources.

The resources are more than adequate to support the abuse mitigation procedures of the .HOTEL registry.

29. Rights Protection Mechanisms

29.1. Rights Protection Mechanisms

Despegar Online SRL (“Despegar”) is firmly committed to the protection of intellectual property rights and to implementing the mandatory rights protection mechanisms contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. Despegar recognizes that although the New gTLD Program includes significant protections beyond those that were mandatory for a number of the current TLDs, a key motivator for Despegar’s selection of Neustar, Inc. (“Neustar”) as its registry services provider is Neustar’s experience in successfully launching a number of TLDs with diverse rights protection mechanisms, including many of the ones required in the Applicant Guidebook. More specifically, Despegar will implement the following rights protection mechanisms in accordance with the Applicant Guidebook as further described below:

Trademark Clearinghouse: a one-stop shop so that trademark holders can protect their trademarks with a single registration;

Sunrise and Trademark Claims processes for the TLD;

Implementation of the Uniform Domain Name Dispute Resolution Policy to address domain names that have been registered and used in bad faith in the TLD;

Uniform Rapid Suspension: A quicker, more efficient, and cheaper alternative to the Uniform Domain Name Dispute Resolution Policy to deal with clear cut cases of cybersquatting;

Implementation of a thick WHOIS, making it easier for rights holders to identify and locate infringing parties.

A. Trademark Clearinghouse Including Sunrise and Trademark Claims

The first mandatory rights protection mechanism (“RPM”) required to be implemented by each new gTLD registry is support for, and interaction with, the Trademark Clearinghouse. The Trademark Clearinghouse is intended to serve as a central repository for information to be authenticated, stored, and disseminated pertaining to the rights of trademark holders. The data maintained in the Clearinghouse will support and facilitate other RPMs, including the mandatory Sunrise Period and Trademark Claims service. Although many of the details of how the Trademark Clearinghouse will interact with each registry operator and registrars, Despegar is actively monitoring the developments of the Implementation Assistance Group (“IAG”) designed to assist ICANN staff in firming up the rules and procedures associated with the policies and technical

requirements for the Trademark Clearinghouse. In addition, Despegar's back-end registry services provider is actively participating in the IAG to ensure that the protections afforded by the Clearinghouse and associated RPMs are feasible and implementable.

Utilizing the Trademark Clearinghouse, all operators of new gTLDs must offer: (i) a Sunrise registration service for at least 30 days during the pre-launch phase, giving eligible trademark owners an early opportunity to register second-level domains in new gTLDs; and (ii) a Trademark Claims service for at least the first 60 days that second-level registrations are open. The trademark claim service is intended to provide clear notice" to a potential registrant of the rights of a trademark owner whose trademark is registered in the clearinghouse. Despegar's registry service provider, Neustar, has already implemented Sunrise and/or Trademark Claims programs for numerous TLDs including .BIZ, .US, .TRAVEL, .TEL, and .CO and will implement the both of these services on behalf of .HOTEL.

Neustar's Experience in Implementing Sunrise and Trademark Claims Processes

In early 2002, Neustar became the first registry operator to launch a successful authenticated Sunrise process. This process permitted qualified trademark owners to pre-register their trademarks as domain names in the .US ccTLD space prior to the opening of the space to the general public. Unlike any other "Sunrise" plans implemented (or proposed before that time), Neustar validated the authenticity of trademark applications and registrations with the United States Patent and Trademark Office (USPTO).

Subsequently, as the back-end registry operator for the .TEL gTLD and the .CO ccTLD, Neustar launched validated Sunrise programs employing processes. These programs are very similar to those that are to be employed by the Trademark Clearinghouse for new gTLDs.

Below is a high-level overview of the implementation of the .CO Sunrise period that demonstrates Neustar's experience and ability to provide a Sunrise service, and an overview of Neustar's experience in implementing a Trademark Claims program to trademark owners for the launch of .BIZ. Neustar's experience in each of these rights protection mechanisms will enable it to seamlessly provide these services on behalf of Despegar as required by ICANN.

Sunrise and .CO

The Sunrise process for .co was divided into two sub-phases:

Local Sunrise giving holders of eligible trademarks that have obtained registered status from the Colombian trademark office the opportunity apply for the .CO domain names corresponding with their marks; and

Global Sunrise program giving holders of eligible registered trademarks of national effect that have obtained a registered status in any country of the world the opportunity apply for the .CO domain names corresponding with their marks for a period of time before registration is open to the public at large.

Like the new gTLD process set forth in the Applicant Guidebook, trademark owners had to have their rights validated by a Clearinghouse provider prior to the registration being accepted by the registry. The Clearinghouse used a defined process for checking the eligibility of the legal rights claimed as the basis of each Sunrise application, using official national trademark databases and submitted documentary evidence.

Applicants and/or their designated agents had the option of interacting directly with the Clearinghouse to ensure their applications were accurate and complete prior to submitting them to the registry pursuant to an optional "Pre-validation Process." Whether or not an applicant was "pre-validated," the applicant had to submit its corresponding domain name application through an accredited registrar. When the Applicant was pre-validated through the Clearinghouse, each was given an associated approval number that it had to supply to the registry. If they were not pre-validated, applicants were required to submit the required trademark information through their registrar to the registry.

At the registry level, Neustar subsequently either delivered the approval number and domain name registration information to the Clearinghouse, or in cases where there was no approval number, trademark information and the domain name registration information that was provided to the Clearinghouse through EPP (as is currently required under the Applicant Guidebook).

Information was then used by the Clearinghouse as either further validation of

those pre-validated applications, or initial validation of those that did not go through pre-validation. If the applicant was validated and its trademark matched the domain name applied for, the Clearinghouse communicated that fact to the Registry via EPP.
When there was only one validated Sunrise application, the application proceeded to registration when .CO launched. If there were multiple validated applications (recognizing that there could be multiple trademark owners sharing the same trademark), those were included in the .CO Sunrise auction process. Neustar tracked all of the information it received and the status of each application and posted that status on a secure website to enable trademark owners to view the status of their Sunrise application.
Although the exact process for the Sunrise program and its interaction between the trademark owner, registry, registrar, and IP Clearinghouse is not completely defined in the Applicant Guidebook and is dependent on the current RFI issued by ICANN in its selection of a Trademark Clearinghouse provider, Neustar's expertise in launching multiple Sunrise processes and its established software will implement a smooth and compliant Sunrise process for the new gTLDs.
Trademark Claims Service Experience
With Neustar's .BIZ TLD launched in 2001, Neustar became the first registry with a Trademark Claims service. Neustar developed the Trademark Claims Service by enabling companies to stake claims to domain names prior to the commencement of live .BIZ domain registrations.
During the Trademark Claims process, Neustar received over 80,000 Trademark Claims from entities around the world. Recognizing that multiple intellectual property owners could have trademark rights in a particular mark, multiple Trademark Claims for the same string were accepted. All applications were logged into a Trademark Claims database managed by Neustar.
The Trademark Claimant was required to provide various information about their trademark rights, including the:
Particular trademark or service mark relied on for the trademark Claim;
Date a trademark application on the mark was filed, if any, on the string of the domain name;
Country where the mark was filed, if applicable;
Registration date, if applicable;
Class or classes of goods and services for which the trademark or service mark was registered;
Name of a contact person with whom to discuss the claimed trademark rights.
Once all Trademark Claims and domain name applications were collected, Neustar then compared the claims contained within the Trademark Claims database with its database of collected domain name applications (DNAs). In the event of a match between a Trademark Claim and a domain name application, an e-mail message was sent to the domain name applicant notifying the applicant of the existing Trademark Claim. The e-mail also stressed that if the applicant chose to continue the application process and was ultimately selected as the registrant, the applicant would be subject to Neustar's dispute proceedings if challenged by the Trademark Claimant for that particular domain name.
The domain name applicant had the option to proceed with the application or cancel the application. Proceeding on an application meant that the applicant wanted to go forward and have the application proceed to registration despite having been notified of an existing Trademark Claim. By choosing to "cancel," the applicant made a decision in light of an existing Trademark Claim notification to not proceed.
If the applicant did not respond to the e-mail notification from Neustar, or elected to cancel the application, the application was not processed. This resulted in making the applicant ineligible to register the actual domain name. If the applicant affirmatively elected to continue the application process after being notified of the Claimant's (or Claimants') alleged trademark rights to the desired domain name, Neustar processed the application.

This process is very similar to the one ultimately adopted by ICANN and incorporated in the latest version of the Applicant Guidebook. Although the collection of Trademark Claims for new gTLDs will be by the Trademark Clearinghouse, many of the aspects of Neustar's Trademark Claims process in

2001 are similar to those in the Applicant Guidebook. This makes Neustar uniquely qualified to implement the new gTLD Trademark Claims process.

B. Uniform Domain Name Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS)

1. UDRP

Prior to joining Neustar, Mr. Neuman was a key contributor to the development of the Uniform Domain Name Dispute Resolution Policy ("UDRP") in 1998. This became the first "Consensus Policy" of ICANN and has been required to be implemented by all domain name registries since that time. The UDRP is intended as an alternative dispute resolution process to transfer domain names from those that have registered and used domain names in bad faith. Although there is not much of an active role that the domain name registry plays in the implementation of the UDRP, Neustar has closely monitored UDRP decisions that have involved the TLDs that it supports and ensures that the decisions are implemented by the registrars supporting its TLDs. When alerted by trademark owners of failures to implement UDRP decisions by its registrars, Neustar either proactively implements the decisions itself or reminds the offending registrar of its obligations to implement the decision.

URS

In response to complaints by trademark owners that the UDRP was too cost prohibitive and slow, and the fact that more than 70 percent of UDRP cases were "clear cut" cases of cybersquatting, ICANN adopted the IRT's recommendation that all new gTLD registries be required, pursuant to their contracts with ICANN, to take part in a Uniform Rapid Suspension system ("URS"). The purpose of the URS is to provide a more cost effective and timely mechanism for brand owners than the UDRP to protect their trademarks and to promote consumer protection on the Internet.

The URS is not meant to address questionable cases of alleged infringement (e.g., use of terms in a generic sense), for anti-competitive purposes, or denial of free speech, but rather for those cases in which there is no genuine contestable issue as to the infringement and abuse that is taking place.

Unlike the UDRP, which requires little involvement of gTLD registries, the URS envisages much more of an active role at the registry level. For example, rather than requiring the registrar to lock down a domain name subject to a UDRP dispute, it is the registry under the URS that must lock the domain within 24 hours of receipt of the complaint from the URS Provider to restrict all changes to the registration data, including transfer and deletion of the domain names.

In addition, in the event of a determination in favor of the complainant, the registry is required to suspend the domain name. This suspension remains for the balance of the registration period and would not resolve the original website. Rather, the nameservers would be redirected to an informational web page provided by the URS Provider about the URS.

Additionally, the WHOIS reflects that the domain name will not be able to be transferred, deleted, or modified for the life of the registration. Finally, there is an option for a successful complainant to extend the registration period for one additional year at commercial rates.

〈Applicant〉 is fully aware of each of these requirements and will have the capability to implement these requirements for new gTLDs. In fact, during the IRT's development of the URS, Neustar began examining the implications of the URS on its registry operations and provided the IRT with feedback on whether the recommendations from the IRT would be feasible for registries to implement. Although there have been a few changes to the URS since the IRT recommendations, Neustar continued to participate in the development of the URS by providing comments to ICANN, many of which were adopted. As a result, Neustar is committed to supporting the URS for all of the registries to which it provides back-end registry services.

C. Implementation of Thick WHOIS

The .HOTEL registry will include a thick WHOIS database as required in Specification 4 of the Registry Agreement. A thick WHOIS provides numerous advantages, including a centralized location of registrant information, the ability to more easily manage and control the accuracy of data, and a consistent user experience.

D. Policies Handling Complaints Regarding Abuse

In addition the rights protection mechanisms addressed above, Despegar will implement a number of measures to handle complaints regarding the abusive registration of domain names in its gTLD as described in its response to Question 28.

Registry Acceptable Use Policy

One of the key policies each new gTLD registry needs to have is an Acceptable Use Policy that clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. The policy must be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the registry to take the appropriate actions based on the type of abuse. This may include locking down the domain name, preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name "on hold," rendering the domain name non-resolvable, transferring to the domain name to another registrar, and⁄or in cases in which the domain name is associated with an existing law enforcement investigation, substituting nameservers to collect information about the DNS queries to assist the investigation. .HOTEL's Acceptable Use Policy, set forth in our response to Question 28, will include prohibitions on phishing, pharming, dissemination of malware, fast flux hosting, hacking, and child pornography. In addition, the policy will include the right of the registry to take action necessary to deny, cancel, suspend, lock, or transfer any registration in violation of the policy.

Monitoring for Malicious Activity

Despegar is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or is part of a real-time investigation by law enforcement.

Once a complaint is received from a trusted source, third party, or detected by the registry, the registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the registry, the sponsoring registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or providing a compelling argument to the registry to keep the name in the zone. If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the registry will place the domain on "ServerHold." Although this action removes the domain name from the gTLD zone, the domain name record still appears in the gTLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

29.2 Safeguards against Unqualified Registrations

As set forth in Despegar's response to Question 28, the proposed use of .HOTEL as gTLD is one in which all of the domain names will initially be registered by Despegar and its qualified subsidiaries and affiliates, thus eliminating the potential of unqualified registrations. Further ensuring that all domain names are only registered by qualified registrants is the fact that these domain names will be registered through Despegar's existing corporate registrar(s), or a similar corporate registrar, which handle(s) Despegar's existing domain name portfolio.

Should Despegar expand the universe of potential registrants in the .HOTEL namespace to include third parties such as licensees and⁄or strategic partners, Despegar intends to offer the following enhanced mechanism to ensure that only qualified registrants have registered in the name space: specifically, a mechanism whereby third parties can submit complaints directly to Despegar (as opposed to ICANN or the sponsoring registrar) about the qualification of a domain name registrant in the .HOTEL namespace. Despegar will then undertake an investigation to either confirm or dismiss the allegation. Despegar reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to resolve any qualification requirements.

If this mechanism, coupled with verification requirements imposed at the registrar level, prove inadequate, Despegar would evaluate implementing an annual sampling of the active zone file to verify registrant qualification as well as WHOIS accuracy. The size of the sampling would be based upon a

meaningful statistical universe and would be subject to change based upon the results of this survey.
29.3 Resourcing Plans
The rights protection mechanisms described in the response above involve a wide range of tasks, procedures, and systems. The responsibility for each mechanism varies based on the specific requirements. In general, the development of applications such as Sunrise and IP claims is the responsibility of the Engineering team, with guidance from the Product Management team. Customer Support and Legal play a critical role in enforcing certain policies such as the rapid suspension process. These teams have years of experience implementing these or similar processes.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development⁄Engineering – 19 employees;
Product Management – four employees;
Customer Support – 12 employees.
Despegar's (2.0 FTE) allocated to registry oversight and compliance should have no problem undertaking these initial functions based upon the closed nature of the registry and the limited zone files size. However, if the number of domain names were to exceed a manageable size, Despegar would consider outsourcing this potential function to a qualified third party that could recognize more efficiencies and economies of scale in implementing these additional safeguard mechanisms.
These combined resources are more than adequate to support the rights protection mechanisms of the .HOTEL registry.

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

Despegar Online SRL and its back-end operator, Neustar, Inc. ("Neustar"), recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The .HOTEL registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.
Neustar's approach to information security starts with comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.
The following is a summary of the security policies that will be used in the .HOTEL registry, including:
Summary of the security policies used in the registry operations;
Description of independent security assessments;
Description of security features that are appropriate for .HOTEL;
List of commitments made to registrants regarding security levels;
All of the security policies and levels described in this section are appropriate for the .HOTEL registry.
30.(a).1 Summary of Security Policies
Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.
The Program defines:
The policies for internal users and its clients to ensure the safe, organized, and fair use of information resources:
The rights that can be expected with that use;

The standards that must be met to effectively comply with policy;
The responsibilities of the owners, maintainers, and users of Neustar's information resources;
Rules and principles used at Neustar to approach information security issues.

The following policies are included in the Program:
Acceptable Use Policy
The Acceptable Use Policy provides the "rules of behavior" covering all Neustar Associates for using Neustar resources or accessing sensitive information.
Information Risk Management Policy
The Information Risk Management Policy describes the requirements for the ongoing information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments; assessments of technologies used to provide information security; and monitoring procedures used to measure policy compliance.
Data Protection Policy
The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.
Third Party Policy
The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.
Security Awareness and Training Policy
The Security Awareness and Training Policy provide the requirements for managing the ongoing awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.
Incident Response Policy
The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting "lessons learned" post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.
Physical and Environmental Controls Policy
The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.
Privacy Policy
Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.
Identity and Access Management Policy
The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.
Network Security Policy
The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.
Platform Security Policy
The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware,

and desktops and laptops owned or operated by Neustar Associates.
Mobile Device Security Policy
The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing, or storing information.
Vulnerability and Threat Management Policy
The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring), and the appropriate ties to the Risk Management Policy.
Monitoring and Audit Policy
The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.
Project and System Development and Maintenance Policy
The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.
30.(a).2 Independent Assessment Reports
Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70), and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management, and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group, and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.
External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts, and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:
A network survey is performed in order to gain a better knowledge of the network that was being tested;
Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase;
Identification of key systems for further exploitation is conducted;
Exploitation of the identified systems is attempted.
Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management’s prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.
30.(a).3 Augmented Security Levels and Capabilities
There are no increased security levels specific for .HOTEL. However, Neustar will provide the same high level of security provided across all of the registries it manages.
A key to Neustar’s operational success is Neustar’s highly structured operations practices. The standards and governance of these processes:
Include annual independent review of information security practices;
Include annual external penetration tests by a third party;
Conform to the ISO 9001 standard (Part of Neustar’s ISO-based Quality Management System);
Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices;
Are aligned with all aspects of ISO IEC 17799;
Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually);
Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4, below.
30.(a).4 Commitments and Security Levels
The .HOTEL registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:
Compliance with High Security Standards;
Security procedures and practices that are in alignment with ISO 17799;
Annual SOC 2 Audits on all critical registry systems;
Annual 3rd Party Penetration Tests;
Annual Sarbanes Oxley Audits;
Highly Developed and Document Security Policies;
Compliance with all provisions described in section 30.(a).4, below, and in the attached security policy document.
Resources necessary for providing information security;
Fully documented security policies;
Annual security training for all operations personnel;
High Levels of Registry Security;
Multiple redundant data centers;
High Availability Design;
Architecture that includes multiple layers of security;
Diversified firewall and networking hardware vendors;
Multi-factor authentication for accessing registry systems;
Physical security access controls;
A 24⁄7 manned Network Operations Center that monitors all systems and applications;
A 24⁄7 manned Security Operations Center that monitors and mitigates DDoS attacks;
DDoS mitigation using traffic scrubbing technologies.

crowell moring

Annex 3.

New gTLD Application Submitted to ICANN by: Spring McCook, LLC

String: hotel

Originally Posted: 13 June 2012

Application ID: 1-1500-16803

Applicant Information

1. Full legal name

Spring McCook, LLC

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

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.

Covered TLD, 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

Covered TLD, 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.

hotel

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 CHAR: 6670

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.

THE .HOTEL 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.

.HOTEL is a TLD attractive to registrants with affinity for or professional interest in the lodging industry. As the term HOTEL is generic and is used all over the world, .HOTEL will be a utilitarian and inclusive TLD. Registrants will come from a very broad and diverse group, including hotel owners, management, investors, suppliers, labor, individual employees, and others interested in the hospitality industry. It would appeal to traditional hotels and the hotel support industry, but also would appeal to less traditional hotels, such as hostels, bed and breakfasts, inns, and others. The TLD also represents a wide and inclusive place for the discussion and exchange of lodging-related topics, including traveler and tour operator ratings, and may be used by schools geared toward the industry. Commensurate with the generic nature of the term, .HOTEL would be operated in a broad, inclusive, and highly secure manner.

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

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

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

OUR PROTECTIONS
Donuts has consulted with and evaluated the ideas of international law enforcement, consumer privacy advocacy organizations, intellectual property interests and other Internet industry groups to create a set of protections that

far exceed those in existing TLDs, and bring to the Internet namespace nearly two dozen new rights and protection mechanisms to raise user safety and protection to a new level.

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

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

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

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

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 CHAR: 8712

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 Standard CHAR: 29543

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. 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 Standard CHAR: 25023

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. 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 Standard CHAR: 19646

1.0. INTRODUCTION

Our Information Security (IS) Program and associated IS Policy, Standards and Procedures apply to all Company 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 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 (EVP) of Information Technology (IT), EVP of Legal & General Counsel, and the EVP of People Operations 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 Company and includes data pertaining to the Company’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⁄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 Board of Directors (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 ensures 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. 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. In addition to the system/ infrastructure security policies and measures described in our response to this Q30, we also provide additional safety and security measures for this string.

These additional measures, which are not required by the applicant guidebookare:

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.

7.0 RESPONSIBILITY OF INFORMATION SECURITY
See Question B Response Section 10.

crowell moring

Annex 4.

New gTLD Application Submitted to ICANN by: dot Hotel Limited

String: hotel

Originally Posted: 13 June 2012

Application ID: 1-1181-77853

Applicant Information

1. Full legal name

dot Hotel Limited

2. Address of the principal place of business

Contact
Information
Redacted

3. Phone number

Contact Information
Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Mr. Geir Andreas Rasmussen

6(b). Title

Chief Executive Officer - Famous Four Media Limited

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

Contact Information Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Brian Winterfeldt

7(b). Title

Partner - Steptoe & Johnson LLP

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

Contact Information Redacted

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited liability company

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

Incorporated under the Gibraltar companies act 1930

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

Attachments are not displayed on this form.

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

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

Domain Venture Partners PCC Limited

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

Applicant Background

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

Domain Management Limited	Director

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

Charles Ashley Richard Melvin	Chief Operating Officer
Iain Simon Roache	Chief Executive Officer
Timothy James Ireton	Chief Financial Officer

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

Domain Venture Partners PCC Limited	Not Applicable

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

Applied-for gTLD string

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

hotel

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

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

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

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

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

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

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

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

Attachments are not displayed on this form.

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

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

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Q16
The Applicant has taken steps to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string (the "String"). The following has been undertaken:

a)The TLD label is valid as specified in relevant technical standards, including: Domain Names: Implementation and Specification (RFC 1035), and Clarifications to the DNS Specification (RFC 2181) and any updates thereto;

b)The TLD label, which is 5 characters long, is well short of the 63 character maximum length;

c) The TLD label is a valid host name, as specified IN: DOD Internet Host Table Specification (RFC 952), Requirements for Internet Hosts — Application and Support (RFC1123), and Application Techniques for Checking and Transformation of Names (RFC 3696), Internationalized Domain Names in Applications (IDNA)(RFCs 5890-5894), and any updates thereto;

d)The TLD label consists entirely of letters (a-z)

The Applicant has evaluated the risks of the TLD experiencing TLD Acceptance issues similar to problems reported in the "Evaluation of the New gTLDs: Policy and Legal Issues" (31⁄08⁄2004) which discussed acceptance issues associated with the year 2000 round of new gTLDs with more than three characters (i.e.,.aero,.coop,.info, .museum, .name). At that time, only one gTLD, .arpa, which is not widely used outside of limited circles – had four letters. As a result, the new gTLDs had compatibility problems with the software used by Internet infrastructure operators and application providers. Some users have recently been reporting issues with the use of .xxx names in applications such as Twitter and Skype where domain names entered from that TLD are not instantly recognized with a hyperlink as more established gTLDs are.

The Applicant's registry backend services provider, Neustar Inc tested the String for potential rendering or operational problems; none were found.

As the String is not an IDN and, therefore, does not contain characters that require mixed right-to-left or left-to-right functions. The applicant has familiarized itself with the requirements and components of the IDNA protocol by reviewing the RFCs and background information found on the ICANN IDN Wiki.

The Applicant tested the String using the ICANN SWORD String Similarity Assessment Tool algorithm. The result of this test is 57. The Applicant considers this to be below the level where issues might occur. Should Registrants experience any acceptance issues the Applicant will have a dedicated Operational and Rendering Team ("ORT") on an on-going basis to assist with operational, rendering issues or any other problems that might arise. The ORT will be in place to assist Registrants with any additional problems that may arise out of new TLD that other applicants may be awarded during this process which could lead to unforeseen string confusion now and in the future.
-end-

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

Mission/Purpose

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

Q18A
Mission and Purpose of .hotel?
The Applicant's mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. Its aim is to become the premier online destination for such creators and their wide range of users. The Applicant will create an Internet space whose central function is to provide a platform for creating, producing and disseminating informative, creative and innovative content that is easily recognizable as pertaining to its stakeholder group. The Applicant is acutely aware of the importance of ICANN's mission in coordinating the global Internet's systems of unique identifiers and ensuring their secure and stable operation. The Applicant's core focus is to create a secure, sustainable, and specialized gTLD, thus supporting ICANN's primary goals for this program in promoting consumer trust, consumer choice, competition and innovation.

Why .hotel?
Worldwide, people use hotels to, amongst other things, celebrate, relax and feel safe and comfortable. Everybody loves to escape to a hotel which best suits their needs, and indeed many enjoy the process of exploring the many possibilities out there. Certainly, the potential for this kind of research has greatly increased with the development of the internet.

However, access to the countless benefits and opportunities which the internet offers, such as finding the perfect hotel for your particular taste, can often be hindered when navigating the ever-expanding sea of irrelevant and sometimes malicious content which also exists.

Thus, the aim of .hotel is to create a blank canvas for the online hotel sector set within a secure environment. The Applicant will achieve this by creating a consolidated, versatile and dedicated space for the hotel sector. As the new space is dedicated to those within this affinity group the Applicant will ensure that consumer trust is promoted. Consequently consumer choice will be augmented as there will be a ready marketplace specifically for hotels and related enterprises to provide their goods and services. All stakeholders within the sector will be able to sample reactions to new ideas, or gather thoughts on the improvements of established ones. This will drive innovation and competition within the hotel sector as there will be new channels available not yet fulfilled by current market offerings. This new environment will cause registrants to seek new and varied ways to separate themselves from the competition.

How will .hotel take shape?
The Applicant believes that the success of the gTLD will be determined largely by the sector's key global stakeholders. These stakeholders will be interested in registering a domain and additionally be motivated to protect their sector from detrimental practices. The Applicant believes that stakeholders should

have the opportunity to influence the gTLD and the way it is governed. Accordingly, the Applicant is establishing a Governance Council ("GC"), consisting of key stakeholders that will serve as an advisory body.

Why Applicant?
The Applicant has substantial combined experience amongst its team in managing global businesses from a financial, legal and operational perspective and an exceptionally strong financial position. The Applicant's Team has previous experience with the entire gTLD life-cycle significantly lowering any launch and ongoing operational risks associated with this application. The Applicant has engaged a world-class Registry services provider to manage the technical infrastructure of the .hotel gTLD. The Applicant is further advised by the leading sector experts in all other areas required to ensure a responsible and successful launch and ongoing management of the gTLD to the benefit of all stakeholders in the ICANN community.

Information for future studies and reviews
The Applicant recognizes the connection of the new gTLD application to the Affirmation of Commitments ("AoC"). To gauge the success of the new gTLD program, the Applicant recognizes that an AoC Review Team will be formed one year after the first delegation. To prepare for this, the ICANN Board resolved the creation of a Working Group to formulate definitions of competition, consumer trust and consumer choice and possible metrics for the future AoC team to consider in its gTLD review. The Applicant understands this effort has not been adopted by the ICANN Board, but many of the proposed metrics may be used to gauge the Applicant's gTLD effectiveness and the gTLD program. The Applicant intends to track costs and benefit metrics to inform future studies and reviews. Proposed definitions are:
- Consumer Trust is defined as the confidence registrants and users have in the consistency of name resolution and the degree of confidence among registrants and users that a TLD Registry operator is fulfilling its proposed purpose and is complying with ICANN policies and applicable national laws.
- Consumer Choice is defined as the range of options available to registrants and users for domain scripts and languages, and for TLDs that offer choices as to the proposed purpose and integrity of their domain name registrants.
- Competition is defined as the quantity, diversity, and the potential for market rivalry of TLDs, TLD Registry operators, and Registrars.

Promoting Competition
Given the proposed definition for competition, the Applicant will attain this by contributing to the quantity and diversity within the Registry Operator space. The Applicant is a new entrant enhancing competition among the providers. The Applicant will promote competition for Registrants by amongst other things:
- Building a healthy growth trend of domain registrations
- Measure migration of content from other TLDs
- Maintain competitive pricing of domains

Promoting consumer trust
.hotel will be developed with consumer trust and satisfaction in mind. After 2 years of operations, the Applicant will conduct a survey to measure consumer trust and consumer satisfaction. This will be used to improve the service. The Applicant will among other things measure the following:
- Service Availability of Critical Registry Systems
- Abuse and Takedown incidents
- Rights protection incidents
- WHOIS data accuracy

Promoting consumer choice
The Applicant intends to promote consumer choice by achieving the following:
- Display of registration requirements and restrictions in the gTLD
- Highly available and geographically diverse Registrar channel
- Effective sunrise and trademark services

Domain names will be available globally, although the Applicant's initial marketing efforts will be predominately directed to potential Registrants represented by the six (6) official languages of the United Nations ("UN Languages"), Arabic, Chinese (Mandarin), English, French, Russian and Spanish. After the initial 2 years it is the Applicant's aim that:
- Registrants globally should have access to Registrar services for the gTLD in at least the six UN Languages
- The gTLD is offered by Registrars covering at least 40 Countries and territories globally

Information on the effectiveness of safeguards
The Applicant takes rights protection and abuse prevention and mitigation very seriously and has developed policies accordingly. Amongst others, the Applicant will collect and evaluate data regarding:
- Effectiveness of the Sunrise process in limiting abusive registration practices
- Effectiveness of the additional Abuse Prevention and Mitigation ("APM") and Rights Protection Mechanisms ("RPM")in limiting abusive registration practices
- Effectiveness of the mandatory APMs and RPMs
-end-

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

Q18b
How do you expect that your proposed gTLD will benefit Registrants, Internet users, and others?

The Applicant's primary intention is to provide a favorable ecosystem for the growth and evolution of the sector. The key to achieving this aim are significant provisions for brand integrity and protection of intellectual property. The Applicant intends to push the boundaries of what can be done through innovative design of the new top level domain, including technologies that capitalize on the sector's needs. A close relationship with the sector's stakeholders is essential to this purpose, and will enable .hotel to grow in response to both Registrant and user needs. The gTLD also contains significant opportunities as a next generation organizational scheme for online content, including provisions for abuse prevention to defend users against malicious registrations. The gTLD has been meticulously designed by a team of industry leaders from an array of different fields. This has enabled the creation of an airtight financial strategy, an inspired technological development plan as well as a close and dynamic relationship with the sector community - all critical needs on the path to the enduring success of the gTLD.

18(b)(i) What is the goal of your proposed gTLD in terms of areas of specialty, service levels, or reputation?

Specialty

The Applicant's key specialty goal is to enable a secure and stable gTLD dedicated to providing global Internet users with a targeted space for subject matter of interest. This gTLD will serve as a home for both Registrants and end-users who feel an affinity with this sector and its associated content. Consequently they will prefer to register domain names, create and post content and seek information in a highly targeted manner.

Allowing users the ability to create a targeted, unique space within the new gTLD will enable them to customize their online offering and presence.
The .hotel gTLD will by itself clearly signal the nature and purpose of such

websites to Internet users.

The applicant intends to actively promote gTLD specific vertical searching in the gTLD for the benefit of Registrants, end-users and other stakeholders. This specialization through Vertical Search will also benefit Internet users seeking authentic online information and products or services as they will no longer have to wade through content completely unrelated to their desired results.

As the gTLD is sector specific it will provide a better context for second level strings allowing for a much higher number of relevant and more conscise domains. This more targeted environment will simplify the user experience across multiple platforms specifically with smartphones and tablets where minimal input is favoured.

Service Levels

The goal of the gTLD Registry is to offer domain name registration services of the highest level, exceeding both ICANN requirements and current sector norms. To achieve these goals, the Applicant has contracted with well established, proven service providers offering the highest possible level of quality in Registry and Registrar services. The expertise of the service providers will ensure that the security and quality of the gTLD will be uncompromised.

The Applicant will further provide the highest level of service to trademark, legal rights owners and second-level domain owners. To achieve this goal the Applicant will be implementing a range of Abuse Prevention and Mitigation policies and procedures. The Applicant is also firmly committed to the protection of Intellectual Property rights and will implement all the mandatory Rights Protection Mechanisms (RPMs) contained in the Applicant Guidebook. Aswell as these The Applicant will further protect the rights of others through the implementation of additional RPMs. The RSP's experience will ensure that the gTLD provides this high level of service to trademark and other legal rights owners to combat abusive and malicious activity within the gTLD.

The Registry will respond to abuse or malicious conduct complaints on a 24⁄7⁄365 basis, respond to requests from governmental and quasi-governmental agencies and law enforcement in a timely manner, and promptly abide by decisions and judgments of UDRP and URS panels, in accordance with ICANN consensus policies.

The Applicant will also provide fast and responsive (24⁄7⁄365) customer support to both Registrars and end-users in a number of languages to assist with general enquiries as well as complaints of abusive or malicious conduct.

Service Levels related to Registry Backend Services

The Applicant will work with Neustar Inc. (hereinafter "RSP") whose extensive experience spans more than a decade. This will ensure delivery of the protected, trusted, and permanently-running Registry infrastructure necessary to reliably host and operate a gTLD. The Applicant will also work with its Registrars to ensure that consumers receive secure, fast, and reliable domain name registration services with a high-level of customer service.

The global DNS network that will be utilised for the resolution of domains in this gTLD has already been operating for over 10 years. It currently delivers DNS resolution for several TLD customers and provides low latency query responses with a 100% DNS uptime service level agreement.

The Applicant will further leverage the RSP's existing DNSSEC infrastructure, capabilities, and experience to provide a robust and standards compliant implementation that ensures DNSSEC services are always available as part of the DNS.

The Shared Registry System ("SRS") to be used for the Applicant's gTLD is a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that has been designed to operate at the highest performance levels. The Applicant's RSP has been able to meet or exceed their SLA requirements nearly every month since it's inception. Their Registry has achieved a 99.997% success rate in meeting SLAs since 2004.

The Applicant's RSP has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the gTLDs that it operates as a Registry Operator for both gTLDs and ccTLDs. The RSP's thick WHOIS solution is production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years.

The Applicant will comply with all the data escrow requirements documented in the Registry Data Escrow ("RyDE") Specification of the Registry Agreement and has a contract in place with Iron Mountain Intellectual Property Management, Inc. ("IM") for RyDE Services. The Applicant and its RSP will in conjunction with Iron Mountain work to ensure that the escrow deposit process is compliant 100% of the time.

Reputation

The Applicant will ensure that the Registry enjoys an excellent reputation through its core focus on creating a secure, sustainable, and specialized gTLD, thus supporting ICANN's primary goals for the new gTLD program in promoting consumer trust, consumer choice, competition and innovation.

The Applicant will strive to become a reputable and successful new gTLD by providing secure, fast and reliable customer service throughout the registration life cycle of all domains in the gTLD.

The Applicant will endeavour to ensure that only non-fraudulent Registrants have domain names in the gTLD via a WHOIS that is searchable, thick and reliable and by being highly responsive to complaints from legal rights owners. The Applicant will further implement an industry leading range of Abuse Prevention and Mitigation policies and procedures as well as RPMs.

The Applicant will provide the financial and operational stability to protect Registrants and ensure the reputation of the Registry. The Applicant has estimated the maximum costs of the critical functions for a three year period by taking the largest single year cost estimate (year 5) and multiplying this by 3. If the calculation used a lower figure the costs estimate would not be at the potential highest amount during the 5 years and the COI instrument would be too small in order to fund the costs of the 5 critical functions for at least 3 years.

The Applicant has decided to commit to providing the highest level of protection to Registrants and Stakeholders by providing ICANN with a COI for the maximum amount as recommended by ICANN in its COI Guidance. This ensures the Registry is reputable, remains conservative and mirrors ICANN's core objectives. In a worst case scenario where the Applicant will not receive any revenue Registrants will be protected not only by the COI, but also by the fact that the Applicant has enough capital to operate for over 3 years.

Question 18(b)(ii) What do you anticipate your proposed gTLD will add to the current space, in terms of competition, differentiation, or innovation?

It is expected that .hotel will provide significant competition for existing and forthcoming gTLDs. The .hotel gTLD will provide a blank canvas of second level domains that will inevitably lead to increased consumer choice and significant innovation from the sector. It will allow Registrants to seek new and varied ways to separate themselves from the competition.

Competition

The Applicant will enhance competition by allowing new Registrants to create new online products and services serving the global marketplace and connecting geographically diverse Registrants and users with a common affinity for the specialized subject matter exemplified by the new gTLD. The new gTLD process and its resulting gTLDs are likely to incentivize top-level domains to improve the security and quality of their online products and services as well as introducing new ones. Thus, this gTLD will benefit consumers by increasing the likelihood of new innovative online products and services.The addition of a new gTLD such as .hotel will also increase competition between existing registries.

The Applicant will promote competition to the benefit of the Registrants by amongst other things:

- Building a healthy growth trend of domain registrations to validate the specialty space
- Promote the migration of sector relevant content from other TLDs
- Maintaining competitive pricing of domains

Differentiation

Currently, there is no gTLD available on the Internet that signifies the specialized products, services, and subject matter encompassed by this gTLD. The gTLD string itself will give a clear indication to website visitors that the site has content relevant to the sector. This will result in the gTLD becoming globally recognizable and viewed as a trusted source of goods, services and information.

Innovation

The gTLD will demonstrate innovation through cutting edge RPMs.

Firstly the Applicant considers the Protection of Intergovernmental Organization ("IGO") names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The Applicant will reserve these strings and only allow for their future release if an IGO on the "reserve list" wishes to make use of the protected string in the gTLD and provides the Applicant with sufficient documentation.

Finally if a Registrant during sunrise and landrush applies to register a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard it will receive a Capital City Claims ("CCC") notification stating this. Subsequently they will have to reply unconditionally agreeing to comply with requirements to protect the reputation of the capital city and any further terms.

These functions will enhance Internet stability, security and will demonstrate to Registrars, Registrants, and end-users of the Registry that abusive or malicious conduct will not be tolerated. They will further contribute significantly to the integrity of the gTLD enabling an environment where stakeholders can innovate with confidence.

Question 18(b)(iii) What goals does your proposed gTLD have in terms of user experience?

The Applicant's goals for the new gTLD are to provide a trusted, secure, and user friendly environment whereby domain names and content relating to its specific affinity group can flourish.

The Applicant believes that the success of the gTLD will be determined by the sector's key stakeholders globally. The Applicant believes that stakeholders should have the opportunity to influence the gTLD and the way it is governed. Accordingly, the Applicant is establishing a Governance Council ("GC"), to serve as an advisory body.

.hotel will be developed with consumer trust, choice and satisfaction in mind and after the initial 2 years, the Applicant will conduct a survey to analyse the gTLD's success in these areas to help further improve the user experience.

To ensure a high level of service the Applicant will further measure:

- Service Availability Targets for the Critical Registry Functions
- The number of abuse incidents and takedowns
- ICANN Compliance
- Rights protection incidents (i.e. UDRP and URS)
- WHOIS data accuracy

The Applicant intends to promote consumer choice by providing the following:

- Highly available and geographically diverse Registrar distribution channel;
- Effective sunrise and trademark services.

Question 18(b)(iv) Provide a complete description of the applicant's intended registration policies in support of the goals listed above.

Registration Policies

The purpose and goal of the Applicant's policies are to ensure competition, fairness, trust and reliability for Registrars, Registrants, the user community, and other stake holders, while maintaining security and stability for the gTLD.

General Policy

Aside from certain start-up mechanisms, all domain names will generally be registered on a first-come, first-served basis. A Trademark Claims service will be offered for the first 90 days of general registration, with the intent of providing clear notice to potential Registrants of the existing rights of trademark owners with registered trademarks in the Trademark Clearinghouse.

Registration Policies

As per ICANN's requirements, the Applicant will be operating both a Sunrise and Landrush period ahead of general availability for the gTLD.

Governance Council

The Applicant is establishing a the GC, to be comprised of key sector stakeholders that will serve as an advisory body. Each GC will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific registration policies,the formulation of guidance on intellectual property and other best practices related to the gTLD.

The Applicant aims to develop an Abuse Prevention and Mitigation Working Group in conjunction with the GC. It will give the Applicant's team advice on abuse preventions and mitigation and how this may effect registration policies. The group will meet to regularly discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them.

Question 18(b)(v) Will your proposed gTLD impose any measures for protecting the privacy or confidential information of Registrants or users? If so, please

describe any such measures.

Data and Privacy Policies

The Applicant shall comply with all the Data, WHOIS, and Privacy requirements in the Applicant Guidebook required by ICANN. The Applicant will take all possible steps to maintain the security and privacy of information or data that it may collect in connection with the planned function and usage of names domains, and will remain in compliance with all confidentiality and security regulations in relevant jurisdictions. This data will be held by the Applicant in accordance with the Registry Agreement that the Applicant will execute with ICANN.

The Applicant has further ensured that its suppliers also understand that keeping information secure and private is of crucial importance and will take all available steps to maintain the security and privacy of information collected from the Applicants in the Sunrise, Landrush and General Availability Phases.

Question 18(b) Describe whether and in what ways outreach and communications will help to achieve your projected benefits.

The Applicant plans on making the gTLD the premier gTLD where individuals and organizations can register, build and maintain websites relating to their specific interest area. Thus, communication with the public and development of an outreach campaign are important goals in connection with the gTLD.

During the gTLD evaluation process, the Applicant plans to conduct a two-to-three month communications campaign aimed at reaching sector stakeholders and informing them of the gTLD's mission and the opportunity to participate in the GC. The communication outreach will include email communications to hundreds of leading sector organizations. It will also be accompanied by the launch of a website for communicating information about the gTLD and allowing interested members of the related sector to express interest in serving on the GC. Other communications efforts, including but not limited to, press releases and social media campaigns may all be initiated to raise further awareness regarding the gTLD.

Shortly after completing the evaluation process and being awarded the gTLD, the Applicant will institute marketing and outreach efforts to inform the public about the new gTLD, its launch schedule, and its intended affinity group. The Applicant will use different outreach and communications methods and venues to get the new gTLD mission and message out to the public, including but not limited to the following: online and print press releases, communications with various media outlets, domain name sector groups, mobile apps and various social media platforms. The GC will be used as a further means of outreach and communication to the Internet community.
-end-

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

Q18C
What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)? What other steps will you take to minimize negative consequences/costs imposed upon consumers?

The Applicant fully appreciates the concerns of ICANN, the GAC and other consumer protection authorities about the need to operate new gTLDs in ways that minimize social costs, consumer vulnerabilities as well as other time and

financial resource costs. To achieve these goals this gTLD will not only employ the ICANN mandated minimum protections, but will also deploy the following innovative protection measures that will put the gTLD at the forefront of addressing these critical issues:

1) Abuse Prevention and Mitigation Policies and Procedures

The Applicant's core mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. To achieve this goal the Applicant will be implementing a range of Abuse Prevention and Mitigation ("APM") policies and procedures.

These Policies and Procedures will include: 1) gTLD APM Plan, 2) Policies and Procedures to Minimize Abusive Registrations ,3) Abuse Point of Contact, 4) Policies for Handling Complaints Regarding the Abuse Policies, 5) Acceptable Use Policy ("AUP"), 6) Proposed Measures for Removal of Orphan Glue Records, 7) Resourcing plans for the initial implementation of, and ongoing maintenance of, the APM initiatives, 8) Registry semi-annual WHOIS verification, 9) Regular monitoring of WHOIS registration data for accuracy and completeness, 10) Registrar WHOIS self-certification, 11) WHOIS data reminder process, 12) Establishing policies and procedures to ensure Registrar compliance, which may include audits, financial incentives, penalties, or other means, 13) Registrar verification of WHOIS, 14) Abuse Response Process, 15) Policies and procedures that define malicious or abusive behaviour, 16) Service Level Requirements for resolution regarding APM issues, 17) Service Level Requirements for Law enforcement requests regarding APM issues, 18) Coordination of APM efforts with sector Groups and Law Enforcement, 19) Rapid takedown and suspension, 20) Controls to Ensure Proper Access to Domain Functions, 21) Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests, 22) Enabling multiple, unique points of contact to request and/or approve update, transfer, and deletion requests, 23) Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted, 24) Additional Mechanism for Protection of Capital City Names, 25) Additional Mechanisms to Protect and Reserve IGO Names, 26) Governance Council Structure, 27) Efforts to increase Registrant Security Awareness, 28) Registrant Disqualification, 29) Restrictions on Proxy Registration Services, 30) Registry Lock. (Q28 for detail)

2) Rights Protection Mechanisms

The Applicant is firmly committed to the protection of Intellectual Property rights and to implementing all the mandatory Rights Protection Mechanisms ("RPMs") contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. Use of domain names that infringe upon the legal rights of others in the gTLD will not be tolerated and preventing abusive registrations is a core objective of the Applicant. The nature of such uses creates security and stability issues for the Registry, Registrars, and Registrants, as well as for users of the Internet in general. The Applicant will minimize time or financial resources costs by preventing abusive registrations and reduce opportunities for behaviours such as phishing or pharming. This will be achieved by implementing comprehensive registration, anti-abuse, and rights protection guidelines as defined in its AUP, as well as innovative additional RPMs such as the Mechanism to Protect IGO Names by blocking second level labels currently present in the .int zone file and the Mechanism for Further Protection of Capital City Names, as described below. In order to identify and address the abusive use of registered names on an ongoing basis, the Applicant will also incorporate and abide by the following RPMs and all other RPMs as specified in Specification 7 of the Registry Agreement and as adopted by the ICANN Board of Directors as ICANN Consensus Policies.

These Rights Protection Mechanisms will among other things include: 1) Trademark Clearinghouse, 2) Applicant's Sunrise Period, 3) Trademark Claims Service , 4) Uniform Domain Name Dispute Resolution Policy, 5) Uniform Rapid

Suspension System, 6) Trademark Post-Delegation Dispute Resolution Procedure, 7) Mechanism to protect IGO Names, 8) Mechanism for Further Protection of Capital City Names, 9) Efforts to promote WHOIS Accuracy, 10) Thick Searchable WHOIS, 11) Semi Annual Audits to Ensure Accurate WHOIS, 12) Policies Handling Complaints Regarding Abuse and Rights Issues, 13) Registry Acceptable Use Policy ("AUP"), 14) Monitoring for Malicious Activity. (Q29 for detail)

3) Governance Council Structure

The Applicant believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed. Accordingly, the Applicant will establish a Governance Council (the "GC") comprised of key sector stakeholders that will serve as an advisory body tasked with defining best practice recommendations for the gTLD space. The Applicant believes that the success of the gTLD will be determined largely by the sector's key stakeholders. Not only will these stakeholders have the primary interest in registering domains in the gTLD, but they will also be motivated to protect the sector from practices that would negatively impact the sector overall. The GC exists to provide guidance on matters related to best practices, intellectual property, authentication, certification, and other matters of importance to the sector and it will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and other best practices related to the gTLD.

4) BITS and Coalition for Online Accountability ("COA") Recommendations

The Applicant will further structure its policies around the BITS and COA Recommendations where relevant to this gTLD. The Applicant's goal is to provide a safe and secure experience for consumers. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial TLDs. The policy comprises of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial gTLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf].

The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy comprises of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http://bit.ly/HuHtmq.

We welcome the recommendations from BITS and the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

5) Registry Operators Startup Plan

The Applicant proposes to implement the following start-up plan so that the new gTLD is introduced in an orderly, transparent and stable manner. This will safeguard competition, fairness, trust and reliability for Registrants, the User Community, ICANN Accredited Registrars, and other Stakeholders.
The Applicant's startup plan is designed to minimize social costs (e.g., time or financial resources costs, as well as various types of consumer

vulnerabilities) by instilling a number of RPMs as well as APMs.
The plan consists of the following multi-phase process that will be executed by the Registry Operator. The timeline for the gTLDs start-up process and associated RPMs in the Applicants gTLD is as follows:

Phase 1 – Sunrise Process:

- Day 1: Sunrise round opens
- Day 60: Sunrise round Closes
- Day 61: Sunrise Allocation Including contention resolution mechanisms opens
- Day 71: Sunrise Allocation contention resolution mechanisms closes

• The following Rights Protection Mechanisms apply:
  a. Trademark Clearinghouse (“TMCH”)
  b. Sunrise Eligibility Requirements (“SER”)
  c. Sunrise Dispute Resolution Policy (“SDRP”)
  d. Uniform Domain Name Dispute Resolution Policy (“UDRP”)
  e. Uniform Rapid Suspension System (”URS”)
  f. Mechanism for the Protection of IGO Names (“PIN”)
  g. Trademark Claims Service (“TCS”) *

Phase 2 – Landrush process:

- Day 72: Landrush opens
- Day 102: Landrush closes
- Day 103: Landrush contention resolution mechanisms opens
- Day 113: Landrush contention resolution mechanisms closes

- The following Rights Protection Mechanisms apply:

  a. UDRP
  b. URS
  c. PIN
  d. Mechanism for Further Protection of Capital City Names (“CCC”)
  e. TCS *

Phase 3 – General Availability/Registrations:

- Day 114: General availability begins

- The following Rights Protection Mechanisms apply:

  a. UDRP
  b. URS
  c. PIN
  d. Trademark Post-Delegation Dispute Resolution Procedure (“PDDRP”)
  e. TCS for the 90 days after day 114 *

* To ease the concerns of trademark owners and mitigate the impact of infringing registrations, the Applicant will be implementing the TCS in all three phases of launch. It is important to note that during the General Availability Phase, the TCS will be used for 90 days, 30 days longer than the ICANN mandated minimum.

18(C)(i) How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come/first-serve basis?

Sunrise and Landrush periods:

During the gTLDs launch period, multiple applications for a particular domain name will be resolved through a Contention Resolution Mechanism (“CRM”) involving auctions. These CRMs will apply to the Sunrise and Landrush

application phases. The CRMs will be conducted by Sedo GMBH, an experienced provider of domain auction services. The mechanisms offered will involve closed auctions where only specific bidders can participate.

During the Applicants Sunrise process, if there are two or more eligible applicants for one domain name string, then the contention will be resolved by auction. Auctions held during the Sunrise phase ("Sunrise Auctions") will be closed and the only bidders will be eligible applicants according to the gTLDs Sunrise eligibility requirements including the TMCH.

During the Applicants Landrush process, if there are two or more eligible applicants for one domain name string, then the contention will be resolved by auction. Auctions held during the Landrush phase ("Landrush Auctions") will be closed and the only bidders will be eligible applicants according to the gTLDs Landrush eligibility requirements.

General Availability:

After the two initial startup phases of the Registry the allocation of domain names will occur on a first-come first-serve basis, taking into account the registries APM and RPM mechanisms.

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

Incentive, Marketing and Outreach Programs

The Applicant will implement a number of incentive, marketing assistance, awareness and PR programs to assist the Registrar channel in providing a sector leading experience to end-users and to provide cost benefits for registrants. The Applicant will work with the global Registrar channel to ensure that the new gTLD offer is clearly visible on registrar sites resulting in an increase in the awareness and in the number of new gTLD registrations. Achieving this visibility requires (1) a clear business case and incentives for registrars to motivate them and (2) mechanisms and assets to make it easy for them to do so.

The Applicant will at the time of launch depending upon market conditions consider incentive programs that will deliver cost benefits to registrants through either the use of advantageous pricing, introductory discounts, bulk registration discounts or other similar methods. The Applicant is aware of Specification 9 – Registry Operator Code of Conduct, and will not directly or indirectly show any preference or provide any special consideration to any Registrar in its marketing efforts.

Example incentive mechanisms the Applicant will provide to the registrars may include:

Marketing Incentives

The Applicant intends to provide expertise, tools and creative assets to the registrars as part of general marketing and co-marketing programs. There is a significant cost saving if the expertise, tools and assets are developed centrally and the costs amortized across the registrar base. Significant cost savings can occur relating to Market Research, Social Customer Relationship Management ("SCRM"), Content Management Systems ("CMS"), Direct Marketing Tools, Marketing Collateral and Analytics Solutions.

The Applicant will employ some or all of the following marketing techniques jointly with registrars globally: (1) Direct Response Print, (2) General Web Marketing, (3) Email campaigns without Incentive, (4) Email with Incentive, (5) Email Marketing - Prospect List, (6) Email Marketing - Sponsored Newsletter, (7) Direct Marketing with Incentive, (8) Web Marketing with Incentive, (9) Viral Marketing (Social, Video, Micro-sites), (10) Develop User Interface

Improvement best practices, (11) Develop Search Engine Optimization best practices, (12) Email Marketing - Registrar List
As an example of a marketing initiative, the Applicant will forward leads to the Registrars "buy" pages as an incentive via the means of Pay-Per-Click ("PPC") search marketing. The Applicant will run multiple PPC campaigns targeting gTLD Registrants and point these to landing pages on the Registrar's websites. Conversions are directly trackable from all PPC campaigns and keywords with a high Click-Through-Rate ("CTR") or conversions will also be leveraged for SEO best practice purposes.

PR and Awareness Incentives:

In addition to the core outreach to the Registrar Channel, the Applicant will engage in a wider outreach to build awareness of the new gTLD with customers, end-users and other stakeholders. The Applicant will engage with a number of high profile individuals associated with the gTLD and will seek to reach end consumers through webcasts, podcasts, traditional broadcast TV as well as radio.

Provision of customer retention toolkits to Registrars:

The Applicant will use propensity modelling to build retention marketing programs to minimize churn whilst building renewal sustainability. The Applicant will develop econometric models designed to measure the likelihood of a customer segment to purchase a product or offer bundle, at a certain point in the relationship lifecycle. They are used to predict the best time, and the best combination of products, to offer to customers who match a certain profile. They are especially effective where there are large numbers of customers and reliable data can be gathered. The Applicant expects that registration volume in the gTLD will provide sufficient data for this modelling.

Measure, benchmark and improve the customer experience:

The Applicant will engage in a program to develop best practice policies related to the customer experience at differing levels of the channel. This will include the entire ecosystem from Registry through Registrar to Resellers and finally end-users. One key metric might be, for example, to reduce the number of clicks to make a purchase equivalent to the most customer friendly e-commerce sites in the world.
The Applicant might, for example, provide website performance tracking tools to registrars, which would benchmark current performance and provide insights into customers' needs and behaviour at the point of purchase.
The Applicant will engage in a Social Customer Relationship Management Program to monitor social media feedback to questions, concerns or other issues. The Applicant will further seek to measure marketing communication expenditure and activity.

Other initiatives that will be considered by the Applicant in its outreach efforts:

(a) Customized Vertical Search App for major mobile platforms.
(b) Designated Twitter channel for the stakeholder community.
(c) Social Media outreach through Facebook and other social media solutions.

Translation into other languages:

At present, the Applicant plans to translate marketing collateral and other content that it considers to have geographically diverse appeal in to the 6 official UN languages, namely Arabic, Chinese (Mandarin), English, French, Russian and Spanish.

18(c)(iii) Note that the Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to

ten years at the discretion of the registrar, but no greater than ten years. Additionally, the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation? If so, please describe your plans.

The Applicant will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator has in excess of ten years of experience managing numerous gTLDs that utilize standard and unique business rules and lifecycles.

Initial registrations of registered names may be made in the registry in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, the registration term for registered names may not exceed ten (10) years. Further the renewal of registered names may be made in one (1) year increments for up to a maximum of ten (10) years. For the avoidance of doubt, renewal of registered names may not extend their registration period beyond ten (10) years from the time of the renewal.

The Applicant plans to review domain name registration rates on an annual basis and will make a determination at that time regarding adjustments, depending upon market factors. Thus, at this time, the Applicant does not plan to make specific guarantees regarding pricing increases.

The Applicant will provide ICANN and each ICANN accredited registrar that has executed the registry-registrar agreement for the gTLD advance written notice of any price increase (including as a result of the elimination of any refunds, rebates, discounts, product tying or other programs which had the effect of reducing the price charged to registrars, unless such refunds, rebates, discounts, product tying or other programs are of a limited duration that is clearly and conspicuously disclosed to the registrar when offered) that complies with the requirements as outlined in the New gTLD Registry Agreement.
-end-

Community-based Designation

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

No

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

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

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

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

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

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

Attachments are not displayed on this form.

Geographic Names

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

No

Protection of Geographic Names

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

Q22
Introduction

The Applicant is aware of the substantial amount of work and effort that has gone into developing policy to address the issue of the reservation and release of geographic names under new gTLDs, including the valuable input from ICANN's Governmental Advisory Committee ("GAC"), the Generic Names Supporting Organisation Reserved Names Working Group, Registry Operators and from elsewhere within the ICANN community.

The Applicant is aware of and understands the requirements set forth in the 11 January 2012 version of the New gTLD Applicant Guidebook (New gTLD Applicant Guidebook) and the GAC advice for protection of geographic names and will implement appropriate measures to ensure that it complies in all respects with ICANN policies and rules regarding both the reservation and release of geographic names at the second level (or other levels).

In addition to this, the Applicant proposes to implement an additional mechanism for the protection of capital city names at the second level that exceeds the requirements in the New gTLD Applicant Guidebook. See description of Capital City Claim service described below.

Reservation of Geographic Names

The initial GAC advice on the protection of geographic names is contained in the GAC document "Principles Regarding New gTLDs" which was presented by the GAC on 28 March 2007. Section 2.7(a) of this document states that new gTLD applicants should "adopt, before the new gTLD is introduced, appropriate procedures for blocking, at no cost and upon demand of governments, public authorities or IGOs, names with national or geographic significance at the second level of any new gTLD".

Specification 5 of the New gTLD Registry Agreement provides further clarity and details the Schedule of Reserved Names at the Second Level (or other levels) in gTLD Registries, whereby the Registry Operator undertakes to reserve certain domain names and prevent them from being registered, delegated or used.

Section 2 of Specification 5 of the New gTLD Registry Agreement requires that all two character labels are initially reserved. This is to avoid conflicts and confusion with existing ccTLD extensions.

Section 5 of Specification 5 of the New gTLD Registry Agreement is more comprehensive and states that:

"5. Country and territory names contained in the following internationally recognized lists shall be initially reserved at the second level and at all other levels within the TLD at which the Registry Operator provides for registrations:

5.1. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union 〈http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU〉 ;

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

5.3. the list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names".

In order to meet these requirements regarding country and territory names, the applicant will maintain and regularly update copies of the aforementioned internationally recognized lists. All labels appearing on those lists, and on any list promulgated or recognized by ICANN for reservation in the future, assuming the corresponding string is unregistered, The Applicant will afford the same protections to new states or cities as they are formed.

The Applicant will reserve all labels appearing on the above referenced lists from time to time, and prevent registration, delegation or use of such names in accordance with ICANN requirements and as described above. In order to ensure that this is implemented correctly, all such labels will be reserved in the name of the applicant in order to prevent their delegation and use.

Release of Reserved Geographic Names

Specification 5 of the New gTLD Registry Agreement also contains provisions for

the release of country and territory names on the basis that agreement is reached with "the applicable government(s), provided, further, that Registry Operator may also propose release of these reservations, subject to review by ICANN's Governmental Advisory Committee and approval by ICANN".

As such the applicant's proposed policy for the release of such reserved terms is cognisant of the review and approval process from the GAC and ICANN.

Based upon a review of the available literature, documentation and guidance, the applicant proposes the following policy to ICANN and the GAC for the potential release of reserved terms under the TLD:

i) Further to the successful evaluation and delegation of the TLD all of the aforementioned labels, as specified under Section 5 of Specification 5 of the New gTLD Registry Agreement will be reserved and thus unavailable for registration during each stage of the launch process including, but not limited to the Sunrise period, the Landrush period through to General registrations.

ii) At any stage during the launch process through to General registrations and beyond, the aforementioned reserved names may only be assigned to the relevant Government or public authority. In such situation they would be assigned using the following process:

a) The corresponding Government or public authority submits a request to the GAC seeking the assignment of the reserved name to themselves and provides the details of the proposed registrant entity for the domain name registration.

b) The GAC will validate it and authenticate the request to establish that is a genuine bona fide request.

c) Once this has been established by the GAC, the request for delegation will be forwarded to the applicant to request the assignment of the domain name. Simultaneously the GAC will also notify ICANN of the GAC approval of the request for the assignment of the domain name.

d) The applicant will issue a unique authorisation code to the proposed registrant entity.

e) The proposed registrant entity will then be able to request the assignment of the domain name to themselves using the authorisation code with an ICANN accredited registrar for the applicant TLD.

In addition to the above, the applicant will also adhere to and implement ICANN policy with regards to the reservation and release of such terms as and when required.

Additional Mechanism for Further Protection of Capital City Names
In parallel with the Landrush Period defined in the answer to question 18, the applicant will implement a Capital City Claim ("CCC") service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is described below:

a) Any prospective domain name registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will automatically receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name corresponds to a capital city name of a country or territory listed in the ISO 3166-1 standard.

b) A potential domain name registrant receiving a CCC notification will have to send a response to the Applicant whereby it will unconditionally comply with the requirements as to representations and warranties required by the Applicant.

c) Unconditional acceptance of the representations and warranties set out in the CCC notification will be a material requirement for a prospective registrant to be eligible to register the domain name in question should said prospective registrant be successful in the Landrush period.

d) Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification listing the names in writing to the GAC Chair.
(see Q28 for more detail)
-end-

Registry Services

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

Q23
23.1 Introduction

The Applicant has elected to partner with Neustar, Inc to provide back-end services for the TLD registry. In making this decision, the Applicant recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the TLD registry. The following section describes the registry services to be provided.

23.2 Standard Technical and Business Components

Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. The Applicant will use Neustar's Registry Services platform to deploy the TLD registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to this TLD:
- Registry-Registrar Shared Registration Service (SRS)
- Extensible Provisioning Protocol (EPP)
- Domain Name System (DNS)
- WHOIS
- DNSSEC
- Data Escrow
- Dissemination of Zone Files using Dynamic Updates
- Access to Bulk Zone Files
- Dynamic WHOIS Updates
- IPv6 Support
- Rights Protection Mechanisms
- Internationalized Domain Names (IDN).

The following is a description of each of the services.

SRS
Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.

EPP
The TLD registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.

DNS
The Applicant will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.

WHOIS
Neustar's existing standard WHOIS solution will be used for the TLD. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy and is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:
Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)
DNSSEC

An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question 43.

Data Escrow
Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:
- Protect against data loss
- Follow industry best practices
- Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure
- Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.
Dissemination of Zone Files using Dynamic Updates
Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.

Access to Bulk Zone Files
The Applicant will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.

Dynamic WHOIS Updates

Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

IPv6 Support
The TLD registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.

Required Rights Protection Mechanisms
The Applicant, will provide all ICANN required Rights Mechanisms, including:
- Trademark Claims Service
- Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
- Registration Restriction Dispute Resolution Procedure (RRDRP)
- UDRP
- URS
- Sunrise service.

More information is presented in the response to Question 29.
Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.

23.3 Unique Services
The Applicant will not be offering services that are unique to this TLD.

23.4 Security or Stability Concerns
All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.
-end-

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Q24
24.1 Introduction
The Applicant has partnered with Neustar, Inc, an experienced TLD registry operator, for the operation of the TLD Registry. The Applicant is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the

art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.
The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

High-level SRS System Description

The SRS to be used for TLD will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, The Applicant is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:
- State-of-the-art, production proven multi-layer design-
- Ability to rapidly and easily scale from low to high volume as a TLD grows
- Fully redundant architecture at two sites
- Support for IDN registrations in compliance with all standards
- Use by over 300 Registrars
- EPP connectivity over IPv6
- Performance being measured using 100% of all production transactions (not sampling).

SRS Systems, Software, Hardware, and Interoperability
The systems and software that the registry operates on are a critical element to providing a high quality of service. If the systems are of poor quality, if they are difficult to maintain and operate, or if the registry personnel are unfamiliar with them, the registry will be prone to outages. Neustar has a decade of experience operating registry infrastructure to extremely high service level requirements. The infrastructure is designed using best of breed systems and software. Much of the application software that performs registry-specific operations was developed by the current engineering team and as a result the team is intimately familiar with its operations.

The architecture is highly scalable and provides the same high level of availability and performance as volumes increase. It combines load balancing technology with scalable server technology to provide a cost effective and efficient method for scaling.

The Registry is able to limit the ability of any one registrar from adversely impacting other registrars by consuming too many resources due to excessive EPP transactions. The system uses network layer 2 level packet shaping to limit the number of simultaneous connections registrars can open to the protocol layer.

All interaction with the Registry is recorded in log files. Log files are generated at each layer of the system. These log files record at a minimum:
- The IP address of the client
- Timestamp
- Transaction Details
- Processing Time.
In addition to logging of each and every transaction with the SRS Neustar maintains audit records, in the database, of all transformational transactions. These audit records allow the Registry, in support of the applicant, to produce a complete history of changes for any domain name.

SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:
- Protocol Layer
- Business Policy Layer
- Database.
Each of the layers is described below.

Protocol Layer
The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.
The EPP servers authenticate against a series of security controls before granting service, as follows:
- The registrar's host exchanges keys to initiate a TLS handshake session with the EPP server.
- The registrar's host must provide credentials to determine proper access levels.
- The registrar's IP address must be preregistered in the network firewalls and traffic-shapers.

Business Policy Layer
The Business Policy Layer is the "brain" of the registry system. Within this layer, the policy engine servers perform rules-based processing as defined through configurable attributes. This process takes individual transactions, applies various validation and policy rules, persists data and dispatches notification through the central database in order to publish to various external systems. External systems fed by the Business Policy Layer include backend processes such as dynamic update of DNS, WHOIS and Billing.

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes.
The SRS today processes over 30 million EPP transactions daily.

Database
The database is the third core component of the SRS. The primary function of the SRS database is to provide highly reliable, persistent storage for all registry information required for domain registration services. The database is highly secure, with access limited to transactions from authenticated registrars, trusted application-server processes, and highly restricted access by the registry database administrators. A full description of the database can be found in response to Question 33.

Figure 24-1 depicts the overall SRS architecture including network components.

Number of Servers
As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the TLD registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.
Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:
- WHOIS
- DNS
- Billing
- Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for TLD.
The SRS includes an "external notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

WHOIS External Notifier
The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.
DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.
Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

Data Warehouse
The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.
Frequency of Synchronization between Servers

The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the external system within 2-3 minutes.

Synchronization Scheme (e.g., hot standby, cold standby)
Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.

Compliance with Specification 6 Section 1.2
The SRS implementation for TLD is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.
Compliance with Specification 10
Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the TLD Registry.The following section describes Neustar’s experience and its capabilities to meet the requirements in the new agreement.

To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics.These measurements are key indicators of the performance and health of the registry. Neustar’s current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.

24.3 Resourcing Plans
The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:
- Development⁄Engineering
- Database Administration
- Systems Administration
- Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.

The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31.Neustar’s SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the TLD registry. The following resources are available from those teams:
Development⁄Engineering – 19 employees

Database Administration- 10 employees
Systems Administration – 24 employees
Network Engineering – 5 employees

The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the TLD registry.
-end-

25. Extensible Provisioning Protocol (EPP)

Q25
25.1 Introduction
The Applicant's back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries.
They deployed one of the first EPP registries in 2001 with the launch of .biz. In 2004, they were the first gTLD to implement EPP 1.0. Over the last ten years Neustar has implemented numerous extensions to meet various unique TLD requirements. Neustar will leverage its extensive experience to ensure that the Applicant is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the TLD registry.
This interface exists within the protocol farm layer as described in Question 24 and is depicted in Figure 25-1.

25.2 EPP Interface
Registrars are provided with two different interfaces for interacting with the registry. Both are EPP based, and both contain all the functionality necessary to provision and manage domain names. The primary mechanism is an EPP interface to connect directly with the registry. This is the interface registrars will use for most of their interactions with the registry.
However, an alternative web GUI (Registry Administration Tool) that can also be used to perform EPP transactions will be provided. The primary use of the Registry Administration Tool is for performing administrative or customer support tasks.
The main features of the EPP implementation are:
- Standards Compliance: The EPP XML interface is compliant to the EPP RFCs. As future EPP RFCs are published or existing RFCs are updated, Neustar makes changes to the implementation keeping in mind of any backward compatibility issues.
- Scalability: The system is deployed keeping in mind that it may be required to grow and shrink the footprint of the Registry system for a particular TLD.
- Fault-tolerance: The EPP servers are deployed in two geographically separate data centers to provide for quick failover capability in case of a major outage in a particular data center. The EPP servers adhere to strict availability requirements defined in the SLAs.
- Configurability: The EPP extensions are built in a way that they can be easily configured to turn on or off for a particular TLD.
- Extensibility: The software is built ground up using object oriented design. This allows for easy extensibility of the software without risking the possibility of the change rippling through the whole application.
- Auditable: The system stores detailed information about EPP transactions from provisioning to DNS and WHOIS publishing. In case of a dispute regarding a name registration, the Registry can provide comprehensive audit information on EPP transactions.
- Security: The system provides IP address based access control, client credential-based authorization test, digital certificate exchange, and connection limiting to the protocol layer.

25.3 Compliance with RFCs and Specifications
The registry-registrar model is described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. As

shown in Table 25-1, EPP is defined by the core set of RFCs that standardize the interface that registrars use to provision domains with the SRS. As a core component of the SRS architecture, the implementation is fully compliant with all EPP RFCs.

Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to EPP. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

Neustar has a long history of providing exceptional service that exceeds all performance specifications. The SRS and EPP interface have been designed to exceed the EPP specifications defined in Specification 10 of the Registry Agreement and profiled in Table 25-2. Evidence of Neustar's ability to perform at these levels can be found in the .biz monthly progress reports found on the ICANN website.

EPP Toolkits
Toolkits, under open source licensing, are freely provided to registrars for interfacing with the SRS. Both Java and C++ toolkits will be provided, along with the accompanying documentation. The Registrar Tool Kit (RTK) is a software development kit (SDK) that supports the development of a registrar software system for registering domain names in the registry using EPP. The SDK consists of software and documentation as described below.

The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol.The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a "dummy" server to aid in the testing of EPP clients.
The accompanying documentation describes the EPP software package hierarchy, the object data model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.3 Proprietary EPP Extensions
The TLD registry will not include proprietary EPP extensions. Neustar has implemented various EPP extensions for both internal and external use in other TLD registries. These extensions use the standard EPP extension framework described in RFC 5730. Table 25-3 provides a list of extensions developed for other TLDs. Should the TLD registry require an EPP extension at some point in the future, the extension will be implemented in compliance with all RFC specifications including RFC 3735.

The full EPP schema to be used in the TLD registry is attached in the document titled "EPP Schema."

25.4 Resourcing Plans
The development and support of EPP is largely the responsibility of the Development⁄Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.
The necessary resources will be pulled from the pool of available resources

described in detail in the response to Question 31. The following resources are available from those teams:
Development⁄Engineering – 19 employees
Quality Assurance - 7 employees.

These resources are more than adequate to support any EPP modification needs of the TLD registry.
-end-

26. Whois

Q26
26.1 Introduction
The Applicant recognizes the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and is firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. The Applicant's back-end registry services provider, Neustar, has extensive experience providing ICANN and RFC-compliant WHOIS services for each of the TLDs that it operates both as a Registry Operator for gTLDs, ccTLDs and back-end registry services provider. As one of the first "thick" registry operators in the gTLD space, Neustar's WHOIS service has been designed from the ground up to display as much information as required by a TLD and respond to a very stringent availability and performance requirement.

Some of the key features of the solution include:

• Fully compliant with all relevant RFCs including 3912
• Production proven, highly flexible, and scalable with a track record of 100% availability over the past 10 years
• Exceeds current and proposed performance specifications
• Supports dynamic updates with the capability of doing bulk updates
• Geographically distributed sites to provide greater stability and performance
• In addition, the thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below.(e.g., IDN, registrant data).

26.2 Software Components
The WHOIS architecture comprises the following components:
• An in-memory database local to each WHOIS node: To provide for the performance needs, the WHOIS data is served from an in-memory database indexed by searchable keys.
• Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.
• Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.
• Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.
• Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.
• Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.
• Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different

information display levels based on user categorization
• SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10
Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement. RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.
Table 26-1 describes Neustar's compliance with Specifications 4 and 10. Neustar ensures compliance with all RFCs through a variety of processes and procedures. Members from the engineering and standards teams actively monitor and participate in the development of RFCs that impact the registry services, including those related to WHOIS. When new RFCs are introduced or existing ones are updated, the team performs a full compliance review of each system impacted by the change. Furthermore, all code releases include a full regression test that includes specific test cases to verify RFC compliance.

26.4 High-level WHOIS System Description
26.4.1 WHOIS Service (port 43)
The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves. The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name's UTF-8 encoded representation along with the Unicode code page.

26.4.2 Web Page for WHOIS queries
In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application. It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:
• Domain names
• Nameservers
• Registrant, Technical and Administrative Contacts
• Registrars
It also provides features not available on the port 43 service.These include:
1. Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources
As described above the WHOIS architecture uses a workflow that decouples the update process from the SRS.This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:
• Firewalls, to protect this sensitive data
• Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
• Packetshaper for source IP address-based bandwidth limiting

• Load balancers to distribute query load
• Multiple WHOIS servers for maximizing the performance of WHOIS service.
The WHOIS service uses HP BL 460C servers, each with 2 X Quad Core CPU and a 64GB of RAM. The existing infrastructure has 6 servers, but is designed to be easily scaled with additional servers should it be needed.
Figure 26-1 depicts the different components of the WHOIS architecture.

26.6 Interconnectivity with Other Registry System
As described in Question 24 about the SRS and further in response to Question 31, "Technical Overview", when an update is made by a registrar that impacts WHOIS data, a trigger is sent to the WHOIS system by the external notifier layer.The update agent processes these updates, transforms the data if necessary and then uses messaging oriented middleware to publish all updates to each WHOIS slave.The local update agent accepts the update and applies it to the local in-memory database. A separate auditor compares the data in WHOIS and the SRS daily and monthly to ensure accuracy of the published data.

26.7 Frequency of Synchronization between Servers Updates from the SRS, through the external notifiers, to the constellation of independent WHOIS slaves happens in real-time via an asynchronous publish⁄subscribe messaging architecture. The updates are guaranteed to be updated in each slave within the required SLA of 95% = 60 minutes. Please note that Neustar's current architecture is built towards the stricter SLAs (95% = 15 minutes) of .BIZ. The vast majority of updates tend to happen within 2-3 minutes.

26.8 Provision for Searchable WHOIS Capabilities
Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will include precautions to avoid abuse and will enable users to search the WHOIS directory using any one or more of the following fields:

• Domain name
• Registrar ID
• Contacts and registrant's name
• Contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.)
• Name server name and name server IP address
• The system will also allow search using non-Latin character sets which are compliant with IDNA specification.

The user will choose one or more search criteria, combine them by Boolean operators (AND, OR, NOT) and provide partial or exact match regular expressions for each of the criterion name-value pairs. The domain names matching the search criteria will be returned to the user.
Figure 26-2 shows an architectural depiction of the new service.

To mitigate the risk of this powerful search service being abused by unscrupulous data miners, a layer of security will be built around the query engine which will allow the registry to identify rogue activities and then take appropriate measures. Potential abuses include, but are not limited to:
• Data Mining
• Unauthorized Access
• Excessive Querying
• Denial of Service Attacks
To mitigate the abuses noted above, Neustar will implement any or all of these mechanisms as appropriate:
• Username-password based authentication
• Certificate based authentication
• Data encryption
• CAPTCHA mechanism to prevent robo invocation of Web query
• Fee-based advanced query capabilities for premium customers.

The searchable WHOIS application will adhere to all privacy laws and policies of the Applicant's registry.

26.9 Resourcing Plans
As with the SRS, the development, customization, and on-going support of the WHOIS service is the responsibility of a combination of technical and operational teams. The primary groups responsible for managing the service include:
• Development⁄Engineering – 19 employees
• Database Administration – 10 employees
• Systems Administration – 24 employees
• Network Engineering – 5 employees
Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will also be involved. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably. The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. Neustar's WHOIS implementation is very mature, and has been in production for over 10 years. As such, very little new development will be required to support the implementation of the Applicant's registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

27. Registration Life Cycle

Q27
27.1 Registration Life Cycle
Introduction
The Applicant will follow the lifecycle and business rules found in the majority of gTLDs today. Our back-end operator, Neustar, has over ten years of experience managing numerous TLDs that utilize standard and unique business rules and lifecycles. This section describes the business rules, registration states, and the overall domain lifecycle that will be used for the TLD.
Domain Lifecycle - Description
The registry will use the EPP 1.0 standard for provisioning domain names, contacts and hosts. Each domain record is comprised of three registry object types: domain, contacts, and hosts
Domains, contacts and hosts may be assigned various EPP defined statuses indicating either a particular state or restriction placed on the object. Some statuses may be applied by the Registrar; other statuses may only be applied by the Registry. Statuses are an integral part of the domain lifecycle and serve the dual purpose of indicating the particular state of the domain and indicating any restrictions placed on the domain. The EPP standard defines 17 statuses, however only 14 of these statuses will be used in the Applicant's registry per the defined TLD business rules.
The following is a brief description of each of the statuses. Server statuses may only be applied by the Registry, and client statuses may be applied by the Registrar.
- OK – Default status applied by the Registry.
- Inactive – Default status applied by the Registry if the domain has less than 2 nameservers.
- PendingCreate – Status applied by the Registry upon processing a successful Create command, and indicates further action is pending. This status will not be used in the TLD registry.
- PendingTransfer – Status applied by the Registry upon processing a successful Transfer request command, and indicates further action is pending.
- PendingDelete – Status applied by the Registry upon processing a successful Delete command that does not result in the immediate deletion of the domain, and indicates further action is pending.
- PendingRenew – Status applied by the Registry upon processing a successful Renew command that does not result in the immediate renewal of the domain, and indicates further action is pending. This status will not be used in the

Applicant's registry.
- PendingUpdate – Status applied by the Registry if an additional action is expected to complete the update, and indicates further action is pending. This status will not be used in the TLD registry.
- Hold – Removes the domain from the DNS zone.
- UpdateProhibited – Prevents the object from being modified by an Update command.
- TransferProhibited – Prevents the object from being transferred to another Registrar by the Transfer command.
- RenewProhibited – Prevents a domain from being renewed by a Renew command.
- DeleteProhibited – Prevents the object from being deleted by a Delete command.

The lifecycle of a domain begins with the registration of the domain. All registrations must follow the EPP standard, as well as the specific business rules described in the response to Question 18 above.Upon registration a domain will either be in an active or inactive state. Domains in an active state are delegated and have their delegation information published to the zone. Inactive domains either have no delegation information or their delegation information in not published in the zone. Following the initial registration of a domain, one of five actions may occur during its lifecycle:
- Domain may be updated
- Domain may be deleted, either within or after the add-grace period
- Domain may be renewed at anytime during the term
- Domain may be auto-renewed by the Registry
- Domain may be transferred to another registrar.

Each of these actions may result in a change in domain state. This is described in more detail in the following section. Every domain must eventually be renewed, auto-renewed, transferred, or deleted. A registrar may apply EPP statuses described above to prevent specific actions such as updates, renewals, transfers, or deletions.

27.1.1 Registration States

Domain Lifecycle – Registration States
- As described above the Applicant's registry will implement a standard domain lifecycle found in most gTLD registries today. There are five possible domain states:
- Active
- Inactive
- Locked
- Pending Transfer
- Pending Delete.

All domains are always in either an Active or Inactive state, and throughout the course of the lifecycle may also be in a Locked, Pending Transfer, and Pending Delete state.Specific conditions such as applied EPP policies and registry business rules will determine whether a domain can be transitioned between states. Additionally, within each state, domains may be subject to various timed events such as grace periods, and notification periods.

Active State

The active state is the normal state of a domain and indicates that delegation data has been provided and the delegation information is published in the zone. A domain in an Active state may also be in the Locked or Pending Transfer states.

Inactive State

The Inactive state indicates that a domain has not been delegated or that the delegation data has not been published to the zone. A domain in an Inactive state may also be in the Locked or Pending Transfer states. By default all domain in the Pending Delete state are also in the Inactive state.

Locked State

The Locked state indicates that certain specified EPP transactions may not be performed to the domain. A domain is considered to be in a Locked state if at

least one restriction has been placed on the domain; however up to eight restrictions may be applied simultaneously. Domains in the Locked state will also be in the Active or Inactive, and under certain conditions may also be in the Pending Transfer or Pending Delete states.

Pending Transfer State
The Pending Transfer state indicates a condition in which there has been a request to transfer the domain from one registrar to another. The domain is placed in the Pending Transfer state for a period of time to allow the current (losing) registrar to approve (ack) or reject (nack) the transfer request. Registrars may only nack requests for reasons specified in the Inter-Registrar Transfer Policy.

Pending Delete State
The Pending Delete State occurs when a Delete command has been sent to the Registry after the first 5 days (120 hours) of registration. The Pending Delete period is 35-days during which the first 30-days the name enters the Redemption Grace Period (RGP) and the last 5-days guarantee that the domain will be purged from the Registry Database and available to public pool for registration on a first come, first serve basis.

27.1.2 Typical Registration Lifecycle Activities
Domain Creation Process
The creation (registration) of domain names is the fundamental registry operation. All other operations are designed to support or compliment a domain creation. The following steps occur when a domain is created.
1. Contact objects are created in the SRS database. The same contact object may be used for each contact type, or they may all be different. If the contacts already exist in the database this step may be skipped.
2. Nameservers are created in the SRS database. Nameservers are not required to complete the registration process; however any domain with less than 2 name servers will not be resolvable.
3. The domain is created using the each of the objects created in the previous steps.In addition, the term and any client statuses may be assigned at the time of creation.
The actual number of EPP transactions needed to complete the registration of a domain name can be as few as one and as many as 40. The latter assumes seven distinct contacts and 13 nameservers, with Check and Create commands submitted for each object.

Update Process
Registry objects may be updated (modified) using the EPP Modify operation.The Update transaction updates the attributes of the object.
For example, the Update operation on a domain name will only allow the following attributes to be updated:
- Domain statuses
- Registrant ID
- Administrative Contact ID
- Billing Contact ID
- Technical Contact ID
- Nameservers
- AuthInfo
- Additional Registrar provided fields.

The Update operation will not modify the details of the contacts. Rather it may be used to associate a different contact object (using the Contact ID) to the domain name. To update the details of the contact object the Update transaction must be applied to the contact itself. For example, if an existing registrant wished to update the postal address, the Registrar would use the Update command to modify the contact object, and not the domain object.
Renew Process
The term of a domain may be extended using the EPP Renew operation. ICANN policy in general establishes the maximum term of a domain name to be 10 years, and the Applicant will not deviating from this policy. A domain may be

renewed ⁄ extended at any point time, even immediately following the initial registration.The only stipulation is that the overall term of the domain name may not exceed 10 years. If a Renew operation is performed with a term value will extend the domain beyond the 10 year limit, the Registry will reject the transaction entirely.
Transfer Process
The EPP Transfer command is used for several domain transfer related operations:
- Initiate a domain transfer
- Cancel a domain transfer
- Approve a domain transfer
- Reject a domain transfer.
To transfer a domain from one Registrar to another the following process is followed:
1. The gaining (new) Registrar submits a Transfer command, which includes the AuthInfo code of the domain name.
2. If the AuthInfo code is valid and the domain is not in a status that does not allow transfers the domain is placed into pendingTransfer status
3. A poll message notifying the losing Registrar of the pending transfer is sent to the Registrar's message queue
4. The domain remains in pendingTransfer status for up to 120 hours, or until the losing (current) Registrar Acks (approves) or Nack (rejects) the transfer request
5. If the losing Registrar has not Acked or Nacked the transfer request within the 120 hour timeframe, the Registry auto-approves the transfer
6. The requesting Registrar may cancel the original request up until the transfer has been completed.

A transfer adds an additional year to the term of the domain. In the event that a transfer will cause the domain to exceed the 10 year maximum term, the Registry will add a partial term up to the 10 year limit. Unlike with the Renew operation, the Registry will not reject a transfer operation.
Deletion Process
A domain may be deleted from the SRS using the EPP Delete operation. The Delete operation will result in either the domain being immediately removed from the database or the domain being placed in pendingDelete status. The outcome is dependent on when the domain is deleted. If the domain is deleted within the first five days (120 hours) of registration, the domain is immediately removed from the database. A deletion at any other time will result in the domain being placed in pendingDelete status and entering the Redemption Grace Period (RGP). Additionally, domains that are deleted within five days (120) hours of any billable (add, renew, transfer) transaction may be deleted for credit.

27.1.3 Applicable Time Elements
The following section explains the time elements that are involved.
Grace Periods
There are six grace periods:
- Add-Delete Grace Period (AGP)
- Renew-Delete Grace Period
- Transfer-Delete Grace Period
- Auto-Renew-Delete Grace Period
- Auto-Renew Grace Period
- Redemption Grace Period (RGP).
The first four grace periods listed above are designed to provide the Registrar with the ability to cancel a revenue transaction (add, renew, or transfer) within a certain period of time and receive a credit for the original transaction.
The following describes each of these grace periods in detail.

Add-Delete Grace Period
The APG is associated with the date the Domain was registered.Domains may be deleted for credit during the initial 120 hours of a registration, and the Registrar will receive a billing credit for the original registration.If the domain is deleted during the Add Grace Period, the domain is dropped from the

database immediately and a credit is applied to the
Registrar's billing account.
Renew
Delete Grace Period
The Renew-Delete Grace Period is associated with the date the Domain was renewed. Domains may be deleted for credit during the 120 hours after a renewal.The grace period is intended to allow Registrars to correct domains that were mistakenly renewed. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP (see below).

Transfer-Delete Grace Period
The Transfer-Delete Grace Period is associated with the date the Domain was transferred to another Registrar. Domains may be deleted for credit during the 120 hours after a transfer. It should be noted that domains that are deleted during the renew grace period will be placed into pendingDelete and will enter the RGP. A deletion of domain after a transfer is not the method used to correct a transfer mistake. Domains that have been erroneously transferred or hijacked by another party can be transferred back to the original registrar through various means including contacting the Registry.

Auto-Renew-Delete Grace Period
The Auto-Renew-Delete Grace Period is associated with the date the Domain was auto-renewed. Domains may be deleted for credit during the 120 hours after an auto-renewal.The grace period is intended to allow Registrars to correct domains that were mistakenly auto-renewed. It should be noted that domains that are deleted during the auto-renew delete grace period will be placed into pendingDelete and will enter the RGP.

Auto-Renew Grace Period
The Auto-Renew Grace Period is a special grace period intended to provide registrants with an extra amount of time, beyond the expiration date, to renew their domain name.The grace period lasts for 45 days from the expiration date of the domain name. Registrars are not required to provide registrants with the full 45 days of the period.

Redemption Grace Period
The RGP is a special grace period that enables Registrars to restore domains that have been inadvertently deleted but are still in pendingDelete status within the Redemption Grace Period. All domains enter the RGP except those deleted during the AGP.
The RGP period is 30 days, during which time the domain may be restored using the EPP RenewDomain command as described below. Following the 30day RGP period the domain will remain in pendingDelete status for an additional five days, during which time the domain may NOT be restored.The domain is released from the SRS, at the end of the 5 day non-restore period. A restore fee applies and is detailed in the Billing Section. A renewal fee will be automatically applied for any domain past expiration.
Neustar has created a unique restoration process that uses the EPP Renew transaction to restore the domain and fulfill all the reporting obligations required under ICANN policy. The following describes the restoration process.

27.2 State Diagram
Figure 27-1 provides a description of the registration lifecycle.
The different states of the lifecycle are active, inactive, locked, pending transfer, and pending delete. Please refer to section 27.1.1 for detail description of each of these states. The lines between the states represent triggers that transition a domain from one state to another.

The details of each trigger are described below:
- Create: Registry receives a create domain EPP command.
- WithNS: The domain has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
- WithOutNS: The domain has not met the minimum number of nameservers required

by registry policy. The domain will not be in the DNS zone.
- Remove Nameservers: Domain's nameserver(s) is removed as part of an update domain EPP command. The total nameserver is below the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
- Add Nameservers: Nameserver(s) has been added to domain as part of an update domain EPP command. The total number of nameservers has met the minimum number of nameservers required by registry policy in order to be published in the DNS zone.
- Delete: Registry receives a delete domain EPP command.
- DeleteAfterGrace: Domain deletion does not fall within the add grace period.
- DeleteWithinAddGrace: Domain deletion falls within add grace period.
- Restore: Domain is restored. Domain goes back to its original state prior to the delete command.
- Transfer: Transfer request EPP command is received.
- Transfer Approve/Cancel/Reject: Transfer requested is approved or cancel or rejected.
- TransferProhibited: The domain is in clientTransferProhibited and/or serverTranferProhibited status. This will cause the transfer request to fail. The domain goes back to its original state.

DeleteProhibited: The domain is in clientDeleteProhibited and/or serverDeleteProhibited status.This will cause the delete command to fail. The domain goes back to its original state.
Note: the locked state is not represented as a distinct state on the diagram as a domain may be in a locked state in combination with any of the other states: inactive, active, pending transfer, or pending delete.

27.2.1 EPP RFC Consistency
As described above, the domain lifecycle is determined by ICANN policy and the EPP RFCs. Neustar has been operating ICANN TLDs for the past 10 years consistent and compliant with all the ICANN policies and related EPP RFCs.
27.3 Resources
The registration lifecycle and associated business rules are largely determined by policy and business requirements; as such the Product Management and Policy teams will play a critical role in working Applicant to determine the precise rules that meet the requirements of the TLD. Implementation of the lifecycle rules will be the responsibility of Development/Engineering team, with testing performed by the Quality Assurance team. Neustar's SRS implementation is very flexible and configurable, and in many case development is not required to support business rule changes.
The Applicant's registry will be using standard lifecycle rules, and as such no customization is anticipated. However should modifications be required in the future, the necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams:
Development/Engineering – 19 employees
Registry Product Management – 4 employees
These resources are more than adequate to support the development needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

28. Abuse Prevention and Mitigation

Q28
The Applicant's core mission and purpose is to create an environment where individuals and companies can interact and express themselves in ways never before seen on the Internet, in a more targeted, secure and stable environment. To achieve this goal the Applicant will be implementing a range of Abuse Prevention and Mitigation policies and procedures. The following is an overview of initiatives undertaken by the Applicant:

1. gTLD Abuse Prevention and Mitigation Implementation Plan
2. Policies and Procedures to Minimize Abusive Registrations
2.1. Implementation plan for Abuse Point of Contact
2.2. Policies for Handling Complaints Regarding the Abuse Policies
2.3. Proposed Measures for Removal of Orphan Glue Records
2.4. Resourcing plans for the initial implementation of, and ongoing maintenance of, the Abuse Prevention and Mitigation initiatives
3. Measures to promote WHOIS accuracy both directly by the Registry and by Registrars via requirements in the Registry-Registrar Agreement ("RRA")):
3.1. Regular monitoring of registration data for accuracy and completeness
3.2. Registrar WHOIS policy self-certification and authentication
3.3. WHOIS data reminder process
3.4. Establishing policies and procedures to ensure Registrar compliance with WHOIS policies, which may include audits, financial incentives, penalties, or other means
3.5. Registry semi-annual WHOIS verification
3.6. Registrar semi-annual verification of WHOIS
4. Policies and procedures that define malicious or abusive behaviour
4.1. Service Level Requirements for resolution
4.2. Service Level Requirements for Law enforcement requests
4.3. Coordination with sector Groups and Law Enforcement
4.4. Rapid takedown and suspension
5. Controls to Ensure Proper Access to Domain Functions:
5.1. Enabling two-factor authentication from Registrants to process update, transfer, and deletion requests;
5.2. Enabling multiple, unique points of contact to request and/or approve update, transfer, and deletion requests;
5.3. Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted
6. Additional Abuse Prevention and Mitigation initiatives
6.1. Additional Mechanism for Protection of Capital City Names
6.2. Additional Mechanisms to Protect and Reserve IGO Names
6.3. Governance Council
7. Resource Planning
7.1. Resource Planning Specific to Backend Registry Activities
7.2. Administrative Services Provider – Famous Four Media Limited
8. ICANN Prescribed Measures
9. Increasing Registrant Security Awareness
10. Registrant Disqualification
11. Restrictions on Proxy Registration Services
12. Registry Lock
13. Scope/Scale Consistency
13.1 Scope/Scale Consistency Specific to Backend Registry Activities
14. Acceptable Use Policy ("AUP")
15. Abuse Response Process

1 gTLD Abuse Prevention and Mitigation Implementation Plan

The Applicant will be implementing a thorough and extensive Abuse Prevention and Mitigation plan, designed to minimise abusive registrations and other detrimental activities that may negatively impact internet users. This plan includes the establishment of a single abuse point of contact, responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the gTLD through all Registrars of record, including those involving a reseller. Details of this point of contact will be clearly published on the Applicant's website. Strong abuse prevention for a new gTLD is an important benefit to the internet community. The Applicant and its backend services provider agree that a Registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the Registry's stakeholders' interest. The Applicant's Backend Services Provider brings extensive experience establishing and implementing registration policies. This

experience will be leveraged to help the Applicant combat abusive and malicious domain activity within the new gTLD space.
One of the key functions of a responsible domain name Registry includes working towards the eradication of domain name abuse including, but not limited to, those resulting from:

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

Further explanation of behaviour considered to be abusive can be found in the Acceptable Use Policy ("AUP") below. Any second-level domain found to be facilitating such behaviours, either upon registration or subsequently, will be subject to rapid compliance action as per the policies outlined below.
The Applicant believes that the success of the gTLD will be determined largely by the sector's broad-spectrum of key stakeholders, who operate globally. The Applicant believes that these stakeholders will be motivated to protect the sector from detrimental practices. The Applicant further believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed, including its abuse prevention policies where appropriate. Accordingly, the Applicant is establishing a Governance Council, to be comprised of key sector stakeholders that will serve as an advisory body. The Governance Council will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and the formulation of guidance on other best practices related to the gTLD. The Applicant aims to develop an Abuse Prevention and Mitigation Working Group in conjunction with the GC. It will give the Applicant's team advice on abuse preventions and mitigation and how this may effect registration policies. The group will meet to regularly discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them. Registrants, Registrars and the Registry will all be involved in this working group.This will likely prove important as the battle with abusive behaviour online must continuously evolve given that abusive behaviour itself mutates and changes. The Governance Council will offer significantly greater opportunities to identify emerging threats and rapidly establish procedures to deal with them than might have been possible simply with a Registry perspective.

2 Policies and Procedures to Minimize Abusive Registrations

Regardless of how well intentioned its user-base is, a Registry must have the policies, resources, personnel, and expertise in place to combat abusive DNS practices. The Applicant's Registry Backend Services Provider is at the forefront of the prevention of such abusive practices. We also believe that a strong program is essential given that Registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet, often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name Registrant, but also to millions of unsuspecting Internet users. Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. The Applicant has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the

Internet or the Registry.

Coalition for Online Accountability ("COA") Recommendations
The Applicant will further structure its policies around the COA Recommendations where relevant to this gTLD. The Applicant's goal is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole. The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy is comprised of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http://bit.ly/HuHtmq. We welcome the recommendations from the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

BITS Recommendations
The Applicant will further structure its policies around the BITS Recommendations where relevant to this gTLD. The Applicant's goal is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole. The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial gTLDs. The policy is comprised of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial gTLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf]. We welcome the recommendations from SSWG and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

2.1 Implementation plan for Abuse Point of Contact

As required by the Registry Agreement, The Applicant will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive matters requiring expedited attention. The Applicant will provide a timely response to abuse complaints concerning all names registered in the gTLD by registrars and their resellers. The Applicant will also provide such information to ICANN prior to the delegation of any domain names in the gTLD. This information shall consist of, at a minimum, a valid name, e-mail address dedicated solely to the handling of malicious conduct complaints and a telephone number and mailing address for the primary contact. The Applicant will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited Registrars, the Applicant's Registry Backend Services Provider shall have an additional point of contact, as it does today, handling requests by Registrars related to abusive domain name practices.

2.2 Policies for Handling Complaints Regarding the Abuse Policies

In order to operate under the new gTLD, Registrants must accept the Acceptable Use Policy. The new gTLD Registry's Acceptable Use Policy clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. In addition, the policy will be incorporated into the applicable Registry-Registrar Agreement ("RRA") and reserve the right for the Registry to take the appropriate actions based on the type of abuse. This will include locking down the domain name preventing any changes to the contact and name server information associated with the domain name, placing the domain name "on hold" rendering the domain name non-resolvable, transferring the domain name to another Registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation. When appropriate, the Applicant will also share information with law enforcement. Each ICANN and gTLD accredited Registrar must agree to pass the Acceptable Use Policy on to its Resellers (if applicable) and ultimately to the gTLD Registrants. The Registry's initial Acceptable Use Policy that the Applicant will use in connection with the gTLD is outlined in a section below.

2.3 Proposed Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN ("SSAC") rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the "dominant use of orphaned glue supports the correct and ordinary operation of the DNS." See http://www.icann.org/en/committees/security/sac048.pdf.
While orphan glue records often support the correct and ordinary operation of the DNS, we understand that such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, botnets, malware, and other abusive behaviours. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS.
Thus, the Registry Operator will remove orphan glue records (as defined at the above link) when provided with evidence in written form that such records are present in connection with malicious conduct. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.
To prevent orphan glue records, the Registry Backend Services Provider performs the following checks before removing a domain or name server:

Checks during domain delete:
- Parent domain delete is not allowed if any other domain in the zone refers to the child name server.
- If the parent domain is the only domain using the child name server, then both the domain and the glue record are removed from the zone.

Check during explicit name server delete:
- The Registry Backend Services Provider confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:
- If the parent domain references the child name server AND if other domains in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain goes out of the zone but the name server glue record does not.
- If no domains reference a name server, then the glue record is removed from the zone file.

2.4 Resourcing plans for the initial implementation of, and ongoing maintenance of, the Abuse Prevention and Mitigation initiatives

Details related to resourcing plans for the initial implementation and ongoing maintenance of the Applicant's abuse plan are provided in Section 7 of this response.

3 Measures to promote WHOIS accuracy both directly by the Registry and by Registrars via requirements in the Registry-Registrar Agreement ("RRA"):

The Applicant acknowledges that ICANN has developed a number of mechanisms over the past decades that are intended to address the issue of inaccurate WHOIS information. Such measures alone have not proven to be sufficient and the Applicant will offer a mechanism whereby third parties can submit complaints directly to the Applicant about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their Registrants. Thirty days after forwarding the complaint to the Registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or any other action was taken. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, the Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies. Further efforts to pre-empt inaccurate WHOIS data made by the Applicant will include:

1) The Applicant will in general discourage the use of proxy registration services. The Applicant understands that there are instances when proxy registrations may be required and will develop best practices for when these instances occur.
2) The Applicant will maintain a web-based form for third parties to submit claims regarding false and⁄or inaccurate WHOIS data and the Applicant will forward credible claims to the Registrar for investigation⁄resolution. The Applicant will follow up to verify that the claim has been satisfactorily resolved. Failure of the Registrar or the Registrant to resolve the problem may result in the Applicant placing the domain name on hold, except in extraordinary circumstances.
3) The Applicant's Registry Backend Services Provider will regularly remind Registrars of their obligation to comply with ICANN's WHOIS Data Reminder Policy. This policy requires Registrars to validate the WHOIS information provided during the registration process, to investigate claims of fraudulent WHOIS information, and to cancel domain name registrations for which WHOIS information is determined to be invalid.
4) WHOIS Verification by Registrars. As part of their Registry-Registrar Agreement all accredited Registrars will be required to revalidate WHOIS data for each record they have registered in the gTLD. The Applicant will leave the ultimate determination of how this procedure takes place to the Registrar, but it must include one of the following approved methods. (1) Email notification (2) Outbound telemarketing effort to the individual listed as the administrative contact for the domain.

3.1 Regular monitoring of registration data for accuracy and completeness

As part of their Registry-Registrar Agreement, all of the Applicant's Registrars will be required to revalidate WHOIS data for each record they have registered on a bi-annual basis. This revalidation will require the Registrar to notify its Registrants in the gTLD about this requirement. While the Applicant reserves the right to suspend domain names that are not verified in a timely manner, the Applicant will engage in other outreach to the Registrant prior to suspending any domain name. As part of the gTLD Abuse reporting system, users can report missing or incomplete WHOIS data via the Registry website. The Applicant will also perform randomized audits of verified WHOIS information to ensure compliance and accuracy.
The Applicant's selected Registry Backend Services Provider has established policies and procedures to encourage Registrar compliance with ICANN's WHOIS accuracy requirements..

3.2 Registrar WHOIS policy self-certification and authentication

The self-certification program consists, in part, of evaluations applied equally to all operational ICANN accredited Registrars for the gTLD and is conducted from time to time throughout the year. Process steps are as follows:
The Registry Backend Services Provider sends an email notification to the ICANN primary Registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.
When the form is submitted, the Registry Backend Services Provider sends the Registrar an automated email confirming that the form was successfully submitted.
The Registry Backend Services Provider reviews the submitted form to ensure the certifications are compliant.
The Registry Backend Services Provider sends the Registrar an email notification if the Registrar is found to be compliant in all areas.
If a review of the response indicates that the Registrar is out of compliance or if the Registry Backend Services Provider has follow-up questions, the Registrar has 10 days to respond to the inquiry.
If the Registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, the Registry Backend Services Provider sends the Registrar a Breach Notice and gives the Registrar 30 days to cure the breach.
If the Registrar does not cure the breach, the Registry Backend Services Provider may terminate the Registry-Registrar Agreement (RRA).

3.3 WHOIS data reminder process.

The Registry Backend Services Provider regularly reminds Registrars of their obligation to comply with ICANN's WHOIS Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/Registrars/wdrp.htm). The Registry Backend Services Provider sends a notice to all Registrars once a year reminding them of their obligation to be diligent in validating the WHOIS information provided during the registration process, to investigate claims of fraudulent WHOIS information, and to cancel domain name registrations for which WHOIS information is determined to be invalid.

3.4 Establishing policies and procedures to ensure Registrar compliance with policies, which may include audits, financial incentives, penalties, or other means.

The Applicant will require as part of the RRA obligations that all accredited Registrars for the gTLD participate in the abuse prevention and mitigation procedures and policies, as well as efforts to improve the accuracy and completeness of WHOIS data. In addition, the Applicant will work to develop an economic incentive program, such as Market Development Funds for Registrars who meet certain SLAs for performance in this area.

3.5 Registry bi-annual WHOIS verification

Additionally, the Applicant will, of its own volition and no less than twice per year, perform a manual review of a random sampling of gTLD domain names in its Registry to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, the Applicant will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their Registrants. Thirty days (30) after forwarding the complaint to the Registrar, the Applicant will reexamine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or some other action was taken. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, The Applicant reserves the right to suspend

the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

3.6 Registrar bi-annual verification of WHOIS

The Applicant will require in the Registry-Registrar Agreement that all accredited Registrars in this gTLD will be obliged to verify WHOIS data for each record they have registered in the gTLD twice a year. Verification can take place via email, phone or any other method to confirm the accuracy of the WHOIS data associated with the domain name. The Applicant will randomly audit WHOIS records to ensure compliance and accuracy. As part of the gTLD Abuse reporting system, users can report missing or incomplete WHOIS data via the Registry website.

4 Policies and procedures that define malicious or abusive behaviour

The applicant has developed policies and procedures that define malicious and abusive behaviour. More information on these policies and procedures can be found in section 14 - Acceptable Use Policy.

4.1 Service Level Requirements for resolution of APM related activities

As pertains to the Applicant’s service level requirements for resolution, we aim to address and potentially rectify the issue as it pertains to all forms of abuse and fraud within 24 hours. Once abusive behaviour is detected or reported, the Applicant’s Customer Service center immediately creates a support ticket in order to monitor and track the issue through resolution. This support team is operational 24⁄7⁄365. A preliminary assessment will be performed in order to determine whether the abuse claim is legitimate. We will classify each incidence of legitimately reported abuse into one of two categories based on the probable severity and immediacy of harm to Registrants and Internet users.

Category 1:
- Probable Severity or Immediacy of Harm: Low
- Examples of types of abusive behaviour: Spam, Malware
- Mitigation steps:
  - Investigate
  - Notify Registrant
- Response times – up to 3 days depending on severity.

Category 2:

- Probable Severity or Immediacy of Harm: Medium to High
- Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control
- Mitigation steps:
  - Suspend domain name
  - Investigate
  - Restore or terminate domain name
- Response times - up to 1 day.

4.2 Service Level Requirements and Coordination regarding Law enforcement APM requests

With the assistance of its Registry Backend Services Provider, the Applicant will meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement, governmental and quasi-governmental agencies of illegal conduct in connection with the use of the gTLD. The Registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such a response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by the Applicant for rapid resolution of

the request.
In the event such request involves any of the activities which can be validated by the Registry and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring Registrar is then given 24 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 24-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on "ServerHold".

4.3 Coordination with sector Groups and Law Enforcement

One of the reasons for which the Registry Backend Services Provider was selected to serve as the Registry Backend Services Provider by the Applicant is the Registry Backend Services Provider's extensive experience and its close working relationship with a number of law enforcement agencies.
The Registry Backend Services Provider is also a participant in a number of sector groups aimed at sharing information amongst key sector players about the abusive registration and use of domain names. Through these organizations the Registry Backend Services Provider shares information with other registries, Registrars, ccTLDs, law enforcement, security professionals, etc. Not only on abusive domain name registrations within its own gTLDs, but also provides information uncovered with respect to domain names in other registries. The Registry Backend Services Provider has often found that rarely are abuses found only in the gTLDs which it manages, but also within other gTLDs. The Registry Backend Services Provider routinely provides this information to the other registries so that it can take the appropriate action.
When executed in accordance with the Registry Agreement, plans will result in compliance with contractual requirements.
The Applicant believes that the proposed collection of protections that involve both proactive and reactive mechanisms outlined above will provide an unmatched level of security and anti-abuse activity within the gTLD. These mechanisms will be part of both the Registry-Registrar Agreement as well as the Registrant Registration Agreement.

4.4 Rapid takedown and suspension system

The Applicant is committed to ensuring that the use of the internet within its Registry is compliant with all relevant laws and legal directions.
The Applicant notes that its role as the Registry operator is not one of judge and jury in all jurisdictions and as such shall direct all complainants to the legal process in the relevant jurisdiction. Upon receiving a valid and enforceable legal judgment or direction it shall comply forthright with the appropriate action which shall include rapid takedown and/or suspension.

5 Controls to Ensure Proper Access to Domain Functions

5.1 Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests;

To ensure proper and secure access to domain functions, the Applicant will develop best practices for its Registrars relating to enabling its Registrants to utilize two factor authentication in its interaction with their Registrar and ultimately the Registry.
The goal of these best practices is to improve domain name security and assist Registrars in protecting the accounts they manage by providing another level of assurance that only authorized registrants can communicate through the registrar with the Registry.

5.2 Enabling multiple, unique points of contact to request and/or approve update, transfer, and deletion requests;

The Applicant will investigate the costs and benefits for introducing a service

whereby a Registrant can elect to designate multiple points of contact for each domain registered to approve changes to a domain before they are effectuated. The Applicant is of the opinion that these additional checks could improve the security of each domain and will look for ways to deploy them in the most cost-effective and user-friendly manner possible.

5.3 Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted

The Applicant will investigate the costs and benefits for introducing a service where by a Registrant can elect to designate multiple points of contact for each domain registered to receive notification of changes to a domain when they are effectuated. The Applicant is of the opinion that these additional checks could improve the security of each domain and will look for ways to deploy them in the most cost-effective and user-friendly manner possible.

6. Additional Abuse Prevention and Mitigation initiatives

6.1 Additional Mechanism for Protection of Capital City Names

In parallel with the Landrush Period defined in the answer to question 18, the Applicant will implement a Capital City Claim (“CCC”) service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is as follows:

1. Any prospective domain name Registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name corresponds to a capital city name of a country or territory listed in the ISO 3166-1 standard.
2. A potential domain name Registrant receiving a CCC notification will have to send a response to the Applicant whereby it will unconditionally comply with the requirements as to representations and warranties required by the Applicant. This will protect the reputation of the capital city as well as any further relevant terms and conditions provided.
3. Unconditional acceptance of the warranties set out in the CCC notification will be a material requirement for a prospective Registrant to be eligible to register the domain name in question should said prospective Registrant be successful in the Landrush period.
4. Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification in writing to the ICANN Government Advisory Committee ("GAC") Chair.

6.2 Additional Mechanisms to Protect and Reserve IGO Names

The Applicant considers the Protection of Intergovernmental Organization ("IGO") names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The .int domain is used for registering organizations established by international treaties between or among national governments and which are widely considered to have independent international legal personality. Thus, the names of these organizations, as with geographic names, can lend an official imprimatur, and if misused, be a source of public confusion or deception.

Reservation of IGO names:

In addition to the mandated and additional reservation of geographic names as provided for in response to Question 22, the Applicant will reserve, and thereby prevent registration of, all names that are registered as second level domains in the most recent .int zone as of 1st November 2012. By doing so, the Applicant will extend additional protection to IGOs that comply with the

current eligibility requirements for the .int gTLD as defined at http://www.iana.org/domains/int/policy/, and that have obtained a second-level registration in the .int zone.

Release of IGO names:

In the future, should any of the IGOs wish to make use of the protected strings, the Registry will release and assign the domain to the respective IGOs using the following process:

a) The IGO submits a request to the Applicant in the hope of the reserved name being assigned to themselves and provides the necessary documentation and details of the proposed registrant entity for the domain name registration.
b) The Applicant will validate and authenticate the request to establish that it is a genuine bona fide request.
c) Once the request has been approved the Applicant will notify the requesting IGO as well as ICANN and the GAC of the approval for the assignment of the domain name.
d) The Applicant will issue a unique authorization code to the proposed IGO registrant.
e) The proposed IGO registrant will then be able to request that the assignment of the domain name is given to them using the authorization code with an ICANN and gTLD accredited Registrar of their choice.

6.3 Governance Council

The Applicant believes that the success of the gTLD will be determined in large by the gTLD's stakeholders. Not only will these stakeholders have the primary interest of registering domains on the gTLD, but they will also be motivated to protect the sector from practices that would negatively impact the sector overall. The Applicant further believes that sector stakeholders should be afforded the opportunity to influence the manner in which the gTLD is governed. Accordingly, the Applicant is establishing a Governance Council (the "GC"), to be comprised of key sector stakeholders that will serve as an advisory body.

The GC will elect its own Board of Directors, which will be responsible for self-governance, the recommendation of sector-specific policies, and the formulation of guidance on intellectual property and other best practices related to the gTLD. This will lead the policy development process of defining how the APM Reporting Website should best reflect the options users, rights holders, etc., have for addressing infringing content or other issues.

7. Resource Planning

7.1 Resource Planning Specific to Backend Registry Activities

Responsibility for abuse mitigation rests with a variety of functional groups. The Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The customer service team also plays an important role in assisting with the investigations, responding to customers, and notifying Registrars of abusive domains. Finally, the Policy/Legal team is responsible for developing the relevant policies and procedures.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources are available from those teams globally distributed:

Customer Support – 12 people
Policy/Legal – 2 people
The resources are more than adequate to support the abuse mitigation procedures of the Registry.

7.2 Administrative Services Provider – Famous Four Media Limited

In addition to those resources set out above provided by the Registry's backend services provider the Applicant's Administration Services Provider shall provide the following extra resources:

- Sunrise Validation Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
- Ongoing Rights Protection Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.

The two key objectives of the Sunrise Validation Team and the Ongoing rights Protection Team (together the "Rights Team") is to:

a. Prevent abusive registrations; and
b. Identify and address the abusive use of registered names on an ongoing basis

Because rights protection is a fundamental core objective of the Applicant it has contracted with its Registry Administration Services Provider that the number of full time personnel made available to the Applicant will be 125% of the estimated requirement to ensure that at all times the Applicant is over resourced in this area. In addition the Applicant shall instruct outside Counsel in any relevant jurisdiction on all matters that are unable to be adequately dealt with by the Sunrise Validation Team or the Ongoing Rights Protection Team.

8. ICANN Prescribed Measures

In accordance with its obligations as a Registry operator, the Applicant will comply with all requirements in the 'gTLD Applicant Guidebook'. In particular, we will comply with the following measures prescribed by ICANN which serve to mitigate the potential for abuse in the gTLD:

- DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage Registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy-to-use manner in order to facilitate deployment by Registrants. Prohibition on Wild Carding as required by section 2.2 of Specification 6 of the Registry Agreement.
- Removal of Orphan Glue records (discussed above in section 4).

9. Increasing Registrant Security Awareness

In order to operate a secure and reliable gTLD, the Applicant will attempt to improve Registrant awareness of the threats of domain name hijacking, Registrant impersonation and fraud, and emphasise the need for and responsibility of Registrants to keep registration (including WHOIS) information accurate. Awareness will be raised by:

- Publishing the necessary information on the Abuse page of our Registry website in the form of presentations and FAQ's.
- Developing and providing to Registrants and resellers Best Common Practices that describe appropriate use and assignment of domain auth Info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

The increase in awareness renders Registrants less susceptible to attacks on their domain names owing to the adoption of the recommended best practices thus serving to mitigate the potential for abuse in the gTLD. The clear responsibility on Registrants to provide and maintain accurate registration information (including WHOIS) further serves to minimise the potential for abusive registrations in the gTLD.

10. Registrant Disqualification

Registrants, their agents or affiliates found through the application of the AUP to have repeatedly engaged in abusive registration may be disqualified from maintaining any registrations or making future registrations. This will be triggered when the Registry Backend Services Provider's records indicate that a Registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy. Registrant disqualification provides an additional disincentive for qualified Registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.
In addition, name servers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.
The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.
For a Registrant to be placed on a list of bad actors, the Applicant will examine the factors noted above, and such determination shall be made by the Applicant at its sole discretion. Once the Applicant determines that a Registrant should be placed onto the list of bad actors, the Applicant will notify its Registry Backend Services Provider, who will be instructed to cause all of the Registrant's second-level domains in the gTLD to resolve to a page which notes that the domain has been disabled for abuse-related reasons. The second-level domains at issue will remain in this state until the expiration of the Registrant's registration term or a decision from a UDRP panel or court of competent jurisdiction requires the transfer or cancellation of such domains.

11. Restrictions on Proxy Registration Services

The Applicant will in general discourage the use of proxy registration services. The Applicant further understands that there are instances when proxy registrations may be required and will develop best practices when these instances occur. Whilst it is understood that implementing measures to promote WHOIS accuracy is necessary to ensure that the Registrant may be tracked down, it is recognised that some Registrants may wish to utilise a proxy registration service to protect their privacy. In the event that Registrars elect to offer such services, the following conditions apply:

- Registrars should take the best practice guidance developed by the Applicant and the Governance Council for the gTLD into account when making Proxy registration services available to its Registrants.
- Registrars must ensure that the actual WHOIS data is obtained from the Registrant and must maintain accurate records of such data.
- Registrars must provide Law Enforcement Agencies ("LEA") with the actual WHOIS data upon receipt of a verified request.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the Abuse page of the Registry website. Individuals and organisations will be encouraged through the Abuse page to report any domain names they believe violate the above restrictions, following which appropriate action may be taken by the Registry Backend Services Provider. Publication of these conditions on the Abuse page of the Registry website ensures that Registrants are aware that despite utilisation of a proxy registration service, actual WHOIS information will be provided to LEA upon request in order to hold Registrants liable for all actions in relation to their domain name.
The certainty that WHOIS information relating to domain names which draw the attention of LEA will be disclosed results in the gTLD being less attractive to those seeking to register domain names for abusive purposes, thus mitigating the potential for abuse in the gTLD.

12. Registry Lock

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. Whilst the Applicant will take efforts to promote the awareness of security amongst Registrants, it is recognised that an added level of security may be provided to Registrants by 'Registry locking' the domain name and thereby prohibiting any updates at the Registry operator level. The Registry lock facility will be offered to all Registrars who may request this service on behalf of their Registrants in order to prevent unintentional transfer, modification or deletion of the domain name. This facility mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update nameservers of a mission-critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name.
Upon receipt of a list of domain names to be placed on Registry lock by an authorised representative from a Registrar, the Registry Backend Services Provider will:

1. Validate that the Registrar is the Registrar of record for the domain names.
2. Set or modify the status codes for the names submitted to serverUpdateProhibited, serverDeleteProhibited and⁄or serverTransferProhibited depending on the request.
3. Record the status of the domain name in the Shared Registration System (SRS).
4. Provide a monthly report to Registrars indicating the names for which the Registry lock service was provided in the previous month.

13. Scope⁄Scale Consistency

The Applicant believes that the proposed collection of protections that involve both proactive and reactive mechanisms outlined above will provide an unmatched level of security and anti-abuse activity within the gTLD and is appropriate for the size and scale of the gTLD.

13.1 Scope⁄Scale Consistency Specific to Backend Registry Activities

The Registry Backend Services Provider is an experienced backend Registry provider that has developed and uses proprietary system scaling models to guide the growth of its gTLD supporting infrastructure. These models direct the Registry Backend Services Provider's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. The Registry Backend Services Provider periodically updates these models to account for the adoption of more capable and cost-effective technologies.
The Registry Backend Services Provider's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, The Registry Backend Services Provider derived the necessary infrastructure required to implement and sustain this gTLD and its APM policies.

14. Acceptable Use Policy

This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its Registrar partners and⁄or that may put the safety and security of any Registrant or user at risk. The process also allows the Registry to take

preventive measures to avoid any such criminal or security threats.
The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert the Registry's Registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.
The following are some (but not all) activities that may be subject to rapid domain compliance:

- Phishing; a criminal activity employing tactics to defraud and defame Internet users via sensitive information with the intent to steal or expose credentials, money or identities. A phishing attack often begins with a spoofed email posing as a trustworthy electronic correspondence that contains hijacked brand names e.g.(financial institutions, credit card companies, e-commerce sites). The language of a phishing email is misleading and persuasive by generating either fear and/or excitement to ultimately lure the recipient to a fraudulent Web site. It is paramount for both the phishing email and Web site to appear credible in order for the attack to influence the recipient. As with the spoofed email, phishers aim to make the associated phishing Web site appear credible. The legitimate target Web site is mirrored to make the fraudulent site look professionally designed. Fake third-party security endorsements, spoofed address bars, and spoofed padlock icons falsely lend credibility to fraudulent sites as well. The persuasive inflammatory language of the email combined with a legitimate looking Web site is used to convince recipients to disclose sensitive information such as passwords, usernames, credit card numbers, social security numbers, account numbers, and mother's maiden name.
- Malware; malicious software that was intentionally developed to infiltrate or damage a computer, mobile device, software and/or operating infrastructure or website without the consent of the owner or authorized party. This includes, amongst others, Viruses, Trojan horses, and worms.
- Domain Name or Domain Theft; the act of changing the registration of a domain name without the permission of its original Registrant.
- Botnet Command and Control; Services run on a domain name that is used to control a collection of compromised computers or "zombies," or to direct Distributed Denial of Service attacks ("DDoS attacks")
- Distribution of Malware; The intentional creation and intentional or unintentional distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, keyloggers, and Trojans.
- Fast Flux Attacks/Hosting; A technique used to shelter Phishing, Pharming, and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP addresses associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find.
- Hacking; the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Pharming; The redirecting of unknown users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Spam; The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the legal age in the relevant jurisdiction.
- Further abusive behaviours include, but are not limited to; Cybersquatting,Front-Running,Gripe Sites, Deceptive and/or Offensive Domain Names, Fake Renewal Notices,Cross-gTLD Registration Scam, Name Spinning, Pay-per-Click, Traffic Diversion, False Affiliation, Domain Kiting / Tasting, fast-flux and 419 scams.

The Registry reserves the right, at its sole discretion, to take any

administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on Registry lock, hold or similar status, that it deems necessary, to its discretion; (1) to protect the integrity and stability of the Registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the Registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by the Registry or any Registrar in connection with a domain name registration. The Registry also reserves the right to place upon Registry lock, hold or similar status a domain name during resolution of a dispute.
Registrants must also agree that they will not use their domain for any purposes which are prohibited by the laws of the jurisdiction(s) in which they do business or any other applicable law. You may not use your domain for any purposes or in any manner which violate a statute, rule or law governing use of the Internet and⁄or electronic commerce, including those statutes related to gaming and⁄or online gambling.
In addition, The Applicant reserves the right to deny attempted registrations from repeat violators of the Registry's Acceptable Use Policy. The Registry's Acceptable Use Policy will incorporate a certification by the Registrant that the domain will be used only for licensed, legitimate activities, and not to facilitate piracy or infringements. The Registrant will be required to accept these terms as part of its registration agreement. The Applicant reserves the right to suspend or cancel a domain for violation of the Registry's Acceptable Use Policy.

15. Abuse Response Process

The Registry is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or are part of a real-time investigation by law enforcement.
Once a complaint is received from a trusted source, third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring Registrar will be notified and be given 48 hours to investigate the activity. This will result in either the take down of the domain name by placing the domain name on hold or the deletion of the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 48-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on "ServerHold". Although this action removes the domain name from the gTLD zone, the domain name record still appears in the gTLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

Additionally, the Applicant will require Registrars to adhere to the following abuse-prevention procedures:

- Each new gTLD accredited Registrar must provide and maintain a valid primary point of contact for abuse complaints. The Applicant will require this as part of the new gTLD RRA.
- The Applicant will explicitly define for Registrars what constitutes abusive behaviour including but not limited to, malicious, negligent, and reckless behaviour. The definition of abusive behaviour will be contained in the AUP and the Applicant will require this as part of the new gTLD RRA.
- Registrars must notify the Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc.),

along with the gTLD impacted. This will be required as part of the new gTLD RRA.
- The Applicant will initiate an Abuse Prevention and Mitigation Working Group. This group will be developed in conjunction with the gTLD Governance Council mentioned above. Its aim will be to give the Applicant's team alternate perspectives about handling incidents of abuse and ways to mitigate them. The group will meet regularly to discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them for the gTLD.
-end-

29. Rights Protection Mechanisms

Q29
The Applicant will be implementing an extensive range of Rights Protection Mechanisms ("RPMs") designed to minimize abusive registrations and other activities that may affect the legal rights of others. The Applicant will implement and comply with all ICANN required RPMs and will in addition implement further measures to better protect the rights of others and minimize abusive registrations.

The following is an overview of Applicant's response to Q29:

1. Rights Protection as a core objective
2. Plans for Rights Protection Mechanisms as part of Start-Up
3. ICANN Mandated Rights Protection Mechanisms
3.1. Trademark Clearinghouse ("TMCH")
3.2. Applicant's Sunrise Period ("ASP")
3.3. Trademark Claims Service ("TCS")
3.4. Uniform Domain Name Dispute Resolution Policy ("UDRP")
3.5. Uniform Rapid Suspension System ("URS")
3.6. Trademark Post-Delegation Dispute Resolution Procedure ("PDDRP")
4. Additional Rights Protection Mechanisms to be implemented by the Applicant on a Voluntary Basis
4.1. Mechanism to protect IGO Names ("PIN")
4.2. Mechanism for Further Protection of Capital City Names ("CCC")
5. Efforts to promote WHOIS Accuracy
5.1. Thick WHOIS
5.2. Semi Annual Audits to Ensure Accurate WHOIS
6. Policies Handling Complaints Regarding Abuse and Rights Issues
7. Registry Acceptable Use Policy("AUP")
8. Monitoring for Malicious Activity
9. Resourcing Plans Specific to Backend Registry Activities
10. Registry Backend Services Provider Experience with Rights Protection Measures

1 Rights Protection as a core objective
The Applicant is firmly committed to the protection of Intellectual Property rights and to implementing the mandatory RPMs contained in the Applicant Guidebook and detailed in Specification 7 of the Registry Agreement. Use of domain names that infringe upon the legal rights of others in the gTLD will not be tolerated and preventing abusive registrations is a core objective of the Applicant. The nature of such uses creates security and stability issues for the Registry, Registrars, and Registrants, as well as for users of the Internet in general. The Applicant will prevent abusive registrations and reduce opportunities for behaviours such as phishing or pharming by implementing comprehensive registration, anti-abuse, and rights protection guidelines as defined in its AUP, as well as innovative additional RPMs such as PIN and the CCC, as described below. In order to identify and address the abusive use of registered names on an ongoing basis, the Applicant will also incorporate and

abide by all mandated RPMs as specified in Specification 7 of the Registry Agreement and as adopted by the ICANN Board of Directors as ICANN Consensus Policies.

2 Plans for Rights Protection Mechanisms as part of Start-Up

The timeline for start-up RPMs in the Applicant's gTLD is as follows:

Phase 1 – Sunrise Process:

- Day 1: Sunrise round opens
- Day 60: Sunrise round Closes
- Day 61: Sunrise Allocation including Contention Resolution Mechanisms ("CRM") opens
- Day 71: Sunrise Allocation CRM closes

- The following Rights Protection Mechanisms apply:
  a. TMCH
  b. Sunrise Eligibility Requirements ("SER")
  c. Sunrise Dispute Resolution Policy ("SDRP")
  d. UDRP
  e. URS
  f. PIN
  g. TCS*

Phase 2 – Landrush process:

- Day 72: Landrush opens
- Day 102: Landrush closes
- Day 103: Landrush CRM opens
- Day 113: Landrush CRM closes

- The following Rights Protection Mechanisms apply:
  a. UDRP
  b. URS
  c. PIN
  d. CCC
  e. TCS*

Phase 3 – General Availability/Registrations:

- Day 114: General availability begins

- The following Rights Protection Mechanisms apply:
  a. UDRP
  b. URS
  c. PIN
  d. PDDRP
  e. TCS* (90 days)

* To ease the concerns of trademark owners and mitigate the impact of infringing registrations, the Applicant will be implementing the Trademark Claims service in all three phases of launch. It is important to note that during the General Availability Phase, the Trademark Claims service will be used for 90 days, 30 days longer than the ICANN mandated minimum.

3 ICANN Mandated Rights Protection Mechanisms

3.1 Trademark Clearinghouse ("TMCH")
The first mandatory RPM required of each new gTLD Registry is support for, and interaction with, the TMCH. The TMCH is intended to serve as a central repository for information pertaining to the rights of trademark holders to be authenticated, stored, and disseminated. The data maintained in the clearinghouse will support and facilitate other RPMs, including the mandatory

Sunrise Period and Trademark Claims service. Although the operational details of how the TMCH will interact with Registry operators and Registrars are still being developed by ICANN, the Applicant is actively monitoring the developments of the Implementation Assistance Group ("IAG"). The IAG is working with ICANN staff to refine and finalize the rules, procedures and technical requirements for the TMCH. In addition, the gTLD's Registry Backend Services Provider is actively participating in the IAG to ensure that the protections afforded by the clearinghouse and associated RPMs are feasible, implementable, and well understood.

Utilizing the TMCH, the Applicant will offer: (i) a Sunrise registration service for 60 days during the pre-launch phase giving eligible trademark owners an early opportunity to register second-level domains in new gTLDs; and (ii) a TCS in all 3 phases of launch including 90 days after phase 3 general availability.

3.2 Applicant's Sunrise Period ("ASP")
All domain names registered during the Sunrise Period will be subject to the Applicant's domain name registration policy. The Applicant will surpass ICANN's mandated minimum by offering a Sunrise Period for sixty (60) days. Owners of trademarks listed in the TMCH that also meet the Applicant's domain name registration requirements will be able to register domain names that are an identical match of their listed trademarks. The Applicant has engaged Famous Four Media Limited ("FFM") as well as other suppliers to assist with this process. The FFM Sunrise Validation Team will consist of a minimum of 11 employees who will work with the Applicant's Trademark Validation Team ("TVT") and outside counsel, to receive and authenticate all Sunrise registrations.

Registrars who are accredited to sell names in the gTLD will ensure that all Sunrise Registrants meet SERs, which will be verified by Clearinghouse data. The proposed SERs include: (i) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use – was submitted to, and validated by, the TMCH; or (b) that have been court-validated; or (c) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008, (ii) optional Registry-elected requirements regarding the international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon submission of all of the required information and documentation, the Registrar will forward the information to the Applicant's TVT for authentication. The Applicant's TVT will review the information and documentation and verify the trademark information and registration eligibility, and notify the potential registrant of any deficiencies.

The Applicant will also incorporate a SDRP. The SRDP will allow challenges to Sunrise Registrations by third parties after acceptance of the registration based on the following four grounds: (i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not have the necessary protections on or before the effective date of the Registry Agreement.

After receiving a Sunrise Complaint, the TVT will review the Complaint to see if the Complainant reasonably asserts a legitimate challenge as defined by the SDRP. If not, the TVT will send a notice to the Complainant that the complaint does not fall within one of the delineated grounds as defined by the SDRP and

that the Applicant considers the matter closed.

If the domain name is found to not meet the SERs, the TVT will immediately suspend the domain name. Thereafter, the TVT will immediately notify the Sunrise Registrant of the suspension of the domain name, the nature of the complaint, and provide the registrant with the option to correct the SER deficiencies in a timely manner or the domain name will be cancelled.

If the registrant responds in a timely manner, the response will be reviewed by the TVT to determine if the SERs are met. If the TVT is satisfied by the registrant's response, the TVT will submit a request to lift the suspension of the domain name and notify the Complainant that their dispute was denied. If the registrant does not respond in a timely manner, the TVT will then notify the Complainant that the complaint was upheld and the registration will be cancelled.

3.3 Trademark Claims Service
The Applicant will offer a TCS in Sunrise and Landrush as well as 90 days of general registration (30 days longer than the ICANN mandated minimum period.) The TCS will be monitored by the TVT. Registrars who are accredited to sell names in the gTLD will be required to review all domain names requested to be registered during the Trademark Claims period to determine if they are an identical match of a trademark that has been filed with the TMCH. A domain name will be considered an identical match when the domain name consists of the complete and identical textual elements of the mark, and includes domain names where (a) spaces contained within a mark are either replaced by hyphens or omitted; (b) certain special characters contained within a trademark are spelled out with appropriate words describing it (e.g., @ and &); and (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain name are either (i) omitted or (ii) replaced by hyphens or underscores. Domain names that are plural forms of a mark or that merely contain a mark as a sub string will not qualify as an identical match.

If the Registrar determines that a prospective domain name registration is identical to a mark registered in the TMCH, the Registrar will be required to ensure that a "Trademark Claims Notice" ("Notice") in English is sent to the prospective registrant of the domain name and a blind copy is sent to the Applicant's TVT. The Notice will provide the prospective registrant with information regarding the trademark referenced in the notice to enhance understanding of the Trademark rights being claimed by the trademark holder. The Notice will be provided in real time without cost to the prospective registrant.

After sending the Notice, the Registrar will require the prospective registrant to specifically warrant within five (5) days that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the notice; and (iii) to the best of the prospective registrant's knowledge that the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice. If the warranty satisfies these requirements, the Registrar will effectuate the registration and notify the Applicant's TVT.

After the effectuation of a registration that is identical to a mark listed in the TMCH, the Registrar will be required to notify the trademark owner that a domain name representing the listed mark has been registered. A copy of this communication will also be sent to the TVT. The trademark owner then has the option of filing a Complaint under the UDRP and the URS against the domain name registrant. The Applicant will require in its relevant agreements that the Registry, Registrar, and registrant all submit to and abide by the determinations of the UDRP and the URS providers.

3.4 Uniform Domain Name Dispute Resolution Policy
The Applicant will abide by all decisions rendered by UdrpP providers and will

specify in its Registry Registrar Agreement ("RRA") and Registration Agreements ("RA") that all parties must also abide by all decisions made by panels in accordance with the UDRP. On the Applicant's Registry website, the Applicant will designate a Rights Protection Contact ("Rights Contact") which will receive all UDRP Complaints and decisions. Upon receipt of a determination, the Rights Contact will work with technical staff at the Registry Backend Services Provider to temporarily lock any domain names as required, and will notify the appropriate Registrar to cancel or transfer all registrations determined by a UDRP panel to be infringing.

3.5 Uniform Rapid Suspension System
The Applicant will implement the URS as provided in the Applicant Guidebook. The Applicant will also specify in its RRA that all parties abide by all decisions made by panels in accordance with the URS. In response to complaints made by trademark owners that the UDRP was too cost prohibitive and slow, and that more than 70 percent of UDRP cases were "clear cut" cases of cybersquatting, ICANN adopted the Implementation Review Team's ("IRT") recommendation that all new gTLD registries be required, pursuant to their contracts with ICANN, to take part in a URS. The purpose of the URS is to provide a more cost effective and timely mechanism for brand owners than the UDRP to protect their trademarks and to promote consumer protection on the Internet.
The URS is not meant to address questionable cases of alleged infringement (e.g., use of terms in a generic sense) or for anti-competitive purposes or denial of free speech, but rather for those cases in which there is no genuine contestable issue as to the infringement and abuse that is taking place. Unlike the UDRP which requires little involvement of gTLD registries, the URS envisages much more of an active role at the Registry-level. For example, rather than requiring the Registrar to lock down a domain name subject to a UDRP dispute, under the URS it is the Registry that must lock the domain within 24 hours of receipt of the complaint from the URS Provider to restrict all changes to the registration data, including transfer and deletion of the domain names.
The Rights Contact will receive all URS Complaints verified by the URS Provider and provide its contact information. In the event of a decision in favour of the complainant, the Registry is required to suspend the domain name. This suspension remains in effect for the remainder of the registration period and would not resolve the original website. The nameservers would be redirected to an informational web page describing the URS Process. The WHOIS for that domain will state that the domain name will not be able to be transferred, deleted, or modified for the life of the registration. Finally, there is an option for a successful complainant to extend the registration period for one additional year at commercial rates. Upon receipt of a decision in the registrant's favour, Rights Contact will notify the Registry operator to unlock the domain name.

3.6 Trademark Post-Delegation Dispute Resolution Procedure ("PDDRP")
The Applicant will participate in all post-delegation procedures required by the Registry agreement, including the PDDRP, and will abide by any decisions of any PDDRP Provider as required in Specification 7 of the Registry Agreement.

4 Additional Rights Protection Mechanisms to be implemented by the Applicant

4.1 Mechanism to Protect IGO Names
The Applicant considers the Protection of Intergovernmental Organization ("IGO") names to be very important. The Applicant will use strings registered as second level domains in the .int gTLD as the basis for this protection. To register in the .int domain, the Registrants must be an IGO that meets the requirements found in RFC 1591. The .int domain is used for registering organizations established by international treaties between or among national governments and which are widely considered to have independent international legal personality. Thus, the names of these organizations, as with geographic names, can lend an official imprimatur, and if misused, be a source of public

confusion or deception.

Reservation of IGO names:
In addition to the mandated and additional reservation of geographic names as provided for in response to Question 22, the Applicant will reserve, and thereby prevent registration of, all names that are registered as second level domains in the most recent .int zone as of 1st November 2012. By doing so, the Applicant will extend additional protection to IGOs that comply with the current eligibility requirements for the .int gTLD as defined at http://www.iana.org/domains/int/policy/, and that have obtained a second-level registration in the .int zone.

Release of IGO names:
In the future, should any of the IGOs wish to make use of the protected strings, the Registry will release and assign the domain to the respective IGOs using the following process:

a)The IGO submits a request to the Applicant in the hope of the reserved name being assigned to themselves and provides the necessary documentation and details of the proposed registrant entity for the domain name registration.
b)The Applicant will validate and authenticate the request to establish that it is a genuine bona fide request.
c)Once the request has been approved the Applicant will notify the requesting IGO as well as ICANN and the GAC of the approval for the assignment of the domain name.
d)The Applicant will issue a unique authorization code to the proposed IGO registrant.
e)The proposed IGO registrant will then be able to request that the assignment of the domain name is given to them using the authorization code with an ICANN and gTLD accredited Registrar of their choice.

4.2 Mechanism for Further Protection of Capital City Names
In parallel with the Landrush Period defined in the answer to question 18, the Applicant will implement a Capital City Claim (CCC) service whereby additional protection will be granted to the capital city names of a country or territory listed in the ISO 3166-1 standard. The CCC process is as follows:
a)Any prospective domain name registrant applying to register a domain name identical to the capital city name of a country or territory listed in the ISO 3166-1 standard will receive from the Applicant a CCC notification highlighting the fact that the applied-for domain name matches a capital city name of a country or territory listed in the ISO 3166-1 standard.
b)A potential domain name registrant receiving a CCC notification will have to send a response to the Applicant whereby they will agree to unconditionally comply with requirements as to representations and warranties required by the Applicant in order to protect the reputation of the capital city as well as any further relevant terms and conditions provided.
c)Unconditional acceptance of the warranties set out in the CCC notification will be a material requirement for a prospective registrant to be eligible to register the domain name in question should said prospective registrant be successful in the Landrush period.
d)Upon registration during the Landrush period of a domain name identical to a capital city name of a country or territory listed in the ISO 3166-1 standard, the Applicant will send a notification in writing to the ICANN Government Advisory Committee ("GAC") Chair.

5 Efforts to promote WHOIS Accuracy

5.1. Thick WHOIS
The Applicant will include a thick searchable WHOIS database both accessible on port 43 as well as on port 80 (http) as required in Specification 4 of the Registry Agreement. A thick WHOIS provides numerous advantages including a centralized location of registrant information, the ability to more easily manage and control the accuracy of data, and a consistent user experience, as

well as greater transparency, a factor critical to rights holders as well as law enforcement in pursuing abusive uses of a domain.

5.2. Bi-Annual Audits to Ensure Accurate WHOIS
The Applicant's TVT will perform a bi-annual review of a random sampling of domain names within the applied-for gTLD to test the accuracy and authenticity of the WHOIS information. Through this review, the Applicant's TVT will examine the WHOIS data for evidence of inaccurate or incomplete Whois information. In the event that such errors or missing information exists, it shall be forwarded to the Registrar, who shall be required to address such deficiencies with its Registrants.

6 Policies Handling Complaints Regarding Abuse and Rights Issues
In addition to the RPMs addressed above, the Applicant will implement a number of measures to handle complaints regarding the abusive registration of domain names in its gTLD that may infringe on the rights of others. Further details are described in the response to Question 28.

7 Registry Acceptable Use Policy
One of the key policies each new gTLD Registry needs is to have an AUP that clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. The policy must be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the Registry to take the appropriate actions based on the type of abuse. This may include locking down the domain name preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name "on hold" rendering the domain name non-resolvable, transferring the domain name to another Registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation. The gTLD's AUP, set forth in our response to Question 28, will include prohibitions on phishing, pharming, dissemination of malware, fast flux hosting, hacking, and child pornography. In addition, the policy will include the right of the Registry to take action necessary to deny, cancel, suspend, lock, or transfer any registration in violation of the policy.
In addition, the Applicant reserves the right to deny attempted registrations from repeat violators of the Registry's AUP. The Registry's AUP will incorporate a certification by the registrant that the domain will be used only for licensed, legitimate activities, and not to facilitate piracy or infringements. The registrant will be required to accept these terms as part of its registration agreement. The Applicant reserves the right to suspend or cancel a domain for violation of the Registry's AUP.

8 Monitoring for Malicious Activity
The Applicant is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the AUP are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security of the gTLD, or are part of a real-time investigation by law enforcement.
Once a complaint is received or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring Registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or to provide a compelling argument to the Registry to keep the name in the zone. If the Registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry may place the domain on "ServerHold". Although this action removes the domain name from the gTLD zone, the domain name record still appears in the gTLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

9 Resourcing Plans Specific to Backend Registry Activities
Responsibility for rights protection rests with a variety of functional groups. The Trademark Validation Team and Sunrise Validation Teams are primarily responsible for investigating claims of marks for domain registration. The customer service team also plays an important role in assisting with the investigations, responding to customers, and notifying Registrars of abusive domains. Finally, the Policy/Legal team is responsible for developing the relevant policies and procedures.

The rights protection mechanisms described in the response above involve a wide range of tasks, procedures, and systems. The responsibility for each mechanism varies based on the specific requirements. In general the development of applications such as sunrise and IP claims is the responsibility of the Engineering team, with guidance from the Product Management team. Customer Support and Legal play a critical role in enforcing certain policies such as the rapid suspension process. These teams have very substantial experience implementing these or similar processes.
The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31. The following resources will be made available:
-Development/Engineering – 19 people
-Product Management - 4 people
-Customer Support – 12 people
The resources are more than adequate to support the rights protection mechanisms of the Registry.

Administrative Services Provider – Famous Four Media Limited

In addition to those resources set out above provided by the Registry's backend services provider the Applicant's Administration Services Provider shall provide the following extra resources:
-Sunrise Validation Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
-Ongoing Rights Protection Team - This shall comprise of 11 employees of which at least one shall be a qualified lawyer specializing in intellectual property law.
The two key objectives of the Sunrise Validation Team and the Ongoing rights Protection Team (together the "Rights Team") is to:

a) Prevent abusive registrations; and
b) Identify and address the abusive use of registered names on an ongoing basis
Given that rights protection is a fundamental core objective of the Applicant it has contracted with its Registry Administration Services Provider that the number of full time personnel made available to the Applicant will be 125% of the estimated requirement to ensure that at all times the Applicant is over resourced in this area.
In addition the Applicant shall instruct outside Counsel in any relevant jurisdiction on all matters that are unable to be adequately dealt with by the Sunrise Validation Team or the Ongoing Rights Protection Team.

10 Registry Backend Services Provider Experience with Rights Protection Measures
The gTLD's Registry Backend Services Provider, Neustar Inc., has already implemented Sunrise and/or Trademark Claims programs for numerous gTLDs including .biz, .us, .travel, .tel and .co and will implement both of these services on behalf of the Applicant.

Neustar's Experience with Sunrise Process:
In early 2002, Neustar became the first Registry operator to successfully launch an authenticated Sunrise process. This process permitted qualified trademark owners to pre-register their trademarks as domain names in the .us gTLD space prior to the opening of the space to the general public. Unlike any other "Sunrise" plans implemented or proposed before that time, Neustar

validated the authenticity of trademark applications and registrations with the United States Patent and Trademark Office (USPTO).
As the back-end Registry operator for the .tel gTLD and the .co ccTLD, Neustar launched a validated Sunrise program employing processes that are very similar to those that will be used by the TMCH for new gTLDs.
Below is a high level overview of the implementation of the .co Sunrise period and the Trademark Claims service that was part of the .biz launch. Neustar's experience in each of these RPMs will enable it to seamlessly provide these services on behalf of the Applicant as required by ICANN.
Sunrise and .co
The Sunrise process for .co was divided into two sub-phases:
- Local Sunrise giving holders of eligible trademarks that have obtained registered status from the Colombian trademark office the opportunity to apply for the .co domain names corresponding with their marks.
- Global Sunrise program giving holders of eligible registered trademarks of national effect, that have obtained a registered status in any country of the world the opportunity to apply for.co domain names corresponding with their marks for a period of time before registration is open to the public at large.
Like the new gTLD process set forth in the Applicant Guidebook, trademark owners had to have their rights validated by a Clearinghouse provider prior to the registration being accepted by the Registry. The Clearinghouse used a defined process for checking the eligibility of the legal rights claimed as the basis of each Sunrise application using official national trademark databases and submitted documentary evidence.
Applicants and⁄or their designated agents had the option of interacting directly with the Clearinghouse to ensure their applications were accurate and complete prior to submitting them to the Registry via an optional "Pre-validation Process". Regardless of whether an Applicant was "pre-validated", all Applicants had to submit their corresponding domain name applications through a .co accredited Registrar. When the Applicant was pre-validated through the Clearinghouse, they were given an associated approval number that had to be supplied to the Registry. If Applicants were not pre-validated, they were required to submit the necessary trademark information through their Registrar to the Registry.
At the Registry level, Neustar, subsequently either delivered the:
- Approval number and domain name registration information to the Clearinghouse, or
- When there was no approval number, trademark information and the domain name registration information was provided to the Clearinghouse through EPP (as is currently required under the Applicant Guidebook).
Information was then used by the Clearinghouse for further validation of those pre-validated applications, or initial validation of those that did not select pre-validation. If the Applicant was validated and their trademark matched the domain name applied for, the Clearinghouse communicated that fact to the Registry via EPP.
When there was only one validated sunrise application for a domain name, the application proceeded to registration when the .co launched. If there were multiple validated applications for the same domain name (recognizing that there could be multiple trademark owners sharing the same trademark), those were processed via the .co Sunrise auction process. Neustar tracked all of the information it received and the status of each application on a secure Website to enable trademark owners to view the status of their Sunrise application.
Although the exact process for the Sunrise program and its interaction with trademark owners, Registry, Registrars, and TMCH is not finalized at the time of the application, Neustar's expertise in launching multiple Sunrise processes and its established software will ensure a smooth and compliant Sunrise process for the new gTLDs.
a) Trademark Claims Service Experience
When Neustar's .biz gTLD launched in 2001, Neustar became the first gTLD with a Trademark Claims ("TC") service. Neustar developed the TC Service by enabling companies to stake claims to domain names prior to the commencement of live .biz domain registrations.
During the TC process, Neustar received over 80,000 TC from entities around the world. Recognizing that multiple intellectual property owners could have

trademark rights in a particular mark, multiple TC for the same string were accepted. All applications were logged into a TC database managed by Neustar. The Trademark Claimant was required to provide various information about their trademark rights, including the:

- Particular trademark or service mark relied on for the trademark Claim
- Date a trademark application on the mark was filed, if any, on the string of the domain name
- Country where the mark was filed, if applicable
- Registration date, if applicable
- Class or classes of goods and services for which the trademark or service mark was registered
- Name of a contact person with whom to discuss the claimed trademark rights.

Once all TC and domain name applications were collected, Neustar then compared the claims contained within the TC database with its database of collected domain name applications (DNAs). In the event of a match between a TC and a domain name application, an e-mail message was sent to the domain name Applicant notifying the Applicant of the existing TC. The e-mail also stressed that if the Applicant chose to continue the application process and was ultimately selected as the registrant, the Applicant would be subject to Neustar's dispute proceedings if challenged by the Trademark Claimant for that particular domain name.

The domain name Applicant had the option to proceed with the application or cancel the application. Proceeding with an application meant that the Applicant wanted the application to proceed to registration despite having been notified of an existing Trademark Claim. By choosing to "cancel," the Applicant made a decision in light of an existing TC notification to not proceed.

If the Applicant did not respond to the e-mail notification from Neustar, or elected to cancel the application, the application was not processed. This prevented the Applicant from registering the actual domain name. If the Applicant affirmatively elected to continue the application process after being notified of the claimant's (or claimants') alleged trademark rights to the desired domain name, Neustar processed the application.

This process is very similar to the one ultimately adopted by ICANN and incorporated in the latest version of the Applicant Guidebook. Although the collection of TC for new gTLDs will be by the TMCH, many of the aspects of Neustar's TC process in 2001 are similar to those in the Applicant Guidebook. This makes Neustar uniquely qualified to implement the new gTLD TC process.

Neustar was also a key contributor to the development of the Uniform Dispute Resolution Policy ("UDRP") in 1998. This became the first "Consensus Policy" of ICANN and has been required to be implemented by all domain name registries since that time. The UDRP is intended to be an alternative dispute resolution process to transfer domain names from those that have registered and used domain names in bad faith. Although there is not much of an active role that the domain name Registry plays in the implementation of the UDRP, Neustar has closely monitored UDRP decisions that have involved the gTLDs which it supports and ensures that the decisions are implemented by the Registrars supporting its gTLDs.

-end-

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

Q30A

The Applicant and our back-end operator, Neustar, recognize the vital need to secure the systems and the integrity of the data in commercial solutions. The Applicant's registry solution will leverage industry-best security practices including the consideration of physical, network, server, and application elements.

The Applicant and Neustar's approach to information security starts with

comprehensive information security policies. These are based on the industry best practices for security including SANS (SysAdmin, Audit, Network, Security) Institute, NIST (National Institute of Standards and Technology), and Center for Internet Security (CIS). Policies are reviewed annually by Neustar's information security team.

The following is a summary of the security policies that will be used in the Applicant's registry, including:

1. Summary of the security policies used in the registry operations
2. Description of independent security assessments
3. Description of security features that are appropriate for the TLD
4. List of commitments made to registrants regarding security levels

All of the security policies and levels described in this section are appropriate for the Applicant's registry.

30(a).1 Summary of Security Policies
Neustar, Inc. has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.

The Program defines:
- The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.
- The rights that can be expected with that use.
- The standards that must be met to effectively comply with policy.
- The responsibilities of the owners, maintainers, and users of Neustar's information resources.
- Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy
The Acceptable Use Policy provides the "rules of behavior" covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy
The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy
The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy
The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy
The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy
The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting "lessons learned" post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy
The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy
Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy
The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy
The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy
The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy
The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy
The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy
The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy

The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.

30.(a).2 Independent Assessment Reports
Neustar IT Operations is subject to yearly Sarbanes-Oxley (SOX), Statement on Auditing Standards #70 (SAS70) and ISO audits. Testing of controls implemented by Neustar management in the areas of access to programs and data, change management and IT Operations are subject to testing by both internal and external SOX and SAS70 audit groups. Audit Findings are communicated to process owners, Quality Management Group and Executive Management. Actions are taken to make process adjustments where required and remediation of issues is monitored by internal audit and QM groups.

External Penetration Test is conducted by a third party on a yearly basis. As authorized by Neustar, the third party performs an external Penetration Test to review potential security weaknesses of network devices and hosts and demonstrate the impact to the environment. The assessment is conducted remotely from the Internet with testing divided into four phases:

- A network survey is performed in order to gain a better knowledge of the network that was being tested
- Vulnerability scanning is initiated with all the hosts that are discovered in the previous phase
- Identification of key systems for further exploitation is conducted
- Exploitation of the identified systems is attempted.

Each phase of the audit is supported by detailed documentation of audit procedures and results. Identified vulnerabilities are classified as high, medium and low risk to facilitate management's prioritization of remediation efforts. Tactical and strategic recommendations are provided to management supported by reference to industry best practices.

30.(a).3 Augmented Security Levels and Capabilities
The Applicant and its backend provider Neustar will provide the same high level of security provided across all of the registries it manages.

A key to Neustar's Operational success is Neustar's highly structured operations practices. The standards and governance of these processes:
- Include annual independent review of information security practices
- Include annual external penetration tests by a third party
- Conform to the ISO 9001 standard (Part of Neustar's ISO-based Quality Management System)
- Are aligned to Information Technology Infrastructure Library (ITIL) and CoBIT best practices
- Are aligned with all aspects of ISO IEC 17799
- Are in compliance with Sarbanes-Oxley (SOX) requirements (audited annually)
- Are focused on continuous process improvement (metrics driven with product scorecards reviewed monthly).

A summary view to Neustar's security policy in alignment with ISO 17799 can be found in section 30.(a).4 below.

BITS Recommendations
The Applicant will structure its policies around the BITS Recommendations where relevant to this gTLD.

The Applicants goal with this gTLD is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the TLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants

and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Security Standards Working Group (SSWG) formed by BITS drafted a set of policy recommendations that should be applied to financial TLDs. The policy comprises of a set of 31 recommendations that should be adopted by ICANN in evaluating any applicant of a financial TLD. The recommendations were posted by BITS in the form of a letter to ICANN at [http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf]

We welcome the recommendations from SSWG and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.
Coalition for Online Accountability ("COA") Recommendations

The Applicant will structure its policies around the COA Recommendations where relevant to this gTLD.

The Applicant's goal with this gTLD is to provide a safe and secure browsing experience for consumers of this gTLD. A domain within this gTLD that is owned, operated by or compromised by a malicious party could cause harm to consumers, to the gTLD's reputation and to the reputation of the Internet itself. As such, additional controls are in place relating to the validity of registrations, as well as additional measures to ensure the correct identity of both Registrants and Registrars relating to changes made within the SRS, and to protecting the integrity of the DNS service as a whole.

The Coalition for Online Accountability have drafted a set of policy recommendations, also endorsed by many other international organizations representing the creative industries, that should be applied to entertainment gTLDs - especially those dependent on copyright protection. The policy comprises of a set of 7 recommendations that should be adopted by ICANN in evaluating any applicant for an entertainment-based gTLD. The recommendations were posted by COA in the form of a letter to ICANN at http://bit.ly/HuHtmq.

We welcome the recommendations from the COA and will strongly consider the recommendations relating to the implementation of this gTLD where considered relevant.

30.(a).4 Commitments and Security Levels
The Applicant's registry commits to high security levels that are consistent with the needs of the TLD. These commitments include:

Compliance with High Security Standards
- Security procedures and practices that are in alignment with ISO 17799
- Annual SOC 2 Audits on all critical registry systems
- Annual 3rd Party Penetration Tests
- Annual Sarbanes Oxley Audits

Highly Developed and Document Security Policies
- Compliance with all provisions described in section 30.(a).4 below and in the attached security policy document.
- Resources necessary for providing information security
- Fully documented security policies
- Annual security training for all operations personnel

High Levels of Registry Security
- Multiple redundant data centers
- High Availability Design
- Architecture that includes multiple layers of security
- Diversified firewall and networking hardware vendors
- Multi-factor authentication for accessing registry systems
- Physical security access controls

- A 24x7 manned Network Operations Center that monitors all systems and applications
- A 24x7 manned Security Operations Center that monitors and mitigates DDoS attacks
- DDoS mitigation using traffic scrubbing technologies

We commit to the following:
– Safeguarding the confidentiality, integrity and availability of registrant's data.
– Compliance with the relevant regulation and legislation with respect to privacy.
– Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
– Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
– That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.
– That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
– A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
– Those emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

The Applicant will further be implementing a thorough and extensive Abuse Prevention and Mitigation plan, designed to minimise abusive registrations and other detrimental activities that may impact security and negatively impact internet users. This plan includes the establishment of a single abuse point of contact, responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the gTLD through all Registrars of record, including those involving a reseller. Details of this point of contact will be clearly published on the Applicant's website.

The following is an overview of certain other security related initiatives undertaken by the Applicant - (see response to Q28 for more detail):

- Policies and Procedures to Minimize Abusive Registrations
- Abuse Point of Contact
- Policies for Handling Complaints Regarding the Abuse Policy
- Acceptable Use Policy ("AUP")
- Measures for removal of Orphan Glue records
- Measures to promote Whois accuracy both directly by the Registry and by Registrars via requirements in the Registry-Registrar Agreement ("RRA")):
    - Registry semi-annual WHOIS verification
    - Authentication of Registrant information as complete and accurate at time of registration.
    - Regular monitoring of registration data for accuracy and completeness
    - Registrar self-certification
    - WHOIS Data reminder processes
    - Establishing policies and procedures to ensure Registrar compliance with policies, which may include audits, financial incentives, penalties, or other means.
    - Registrar verification of WHOIS
- Policies and procedures that define malicious or abusive behavior
- Abuse Response Process
    - Service Levels Requirements for Resolution
    - Service Levels Requirements for Law enforcement Requests
    - Coordination with Industry Groups and Law Enforcement
- Controls to ensure proper access to domain functions:

- Enabling two-factor authentication from Registrants to process update, transfers, and deletion requests;
- Enabling multiple, unique points of contact to request and/or approve update, transfer, and deletion requests;
- Enabling the notification of multiple, unique points of contact when a domain has been updated, transferred, or deleted

- Additional Abuse Prevention and Mitigation initiatives:
  - Additional Mechanism for Protection of Capital City Names
  - Additional Mechanisms to Protect and Reserve IGO Names
- Increasing Registrant Security Awareness
- Registrant Disqualification
- Restrictions on Proxy Registration Services
- Registry Lock Option

Resourcing Plans

The development and maintenance of the information security policies and practices are the primary responsibility of the Information Security team. As described in response to Question 31, the information security team is comprised of highly trained security professionals. They establish security policies, actively monitor for intrusions and other nefarious activity, and ensure that all Neustar employees are adhering to Neustar's security policies and best practices. These engineers ensure that the registry data is not compromised in any way.
The necessary resources to support all of the registry's security needs will be pulled from the pool of resources described in detail in the response to Question 31. The following resources are available from the team:

- Information Security - 16 employees

The resources are more than adequate to support the database needs of all the TLDs operated by Neustar, including the Applicant's registry.
-end-

crowell moring

Annex 5.

New gTLD Application Submitted to ICANN by: Fegistry, LLC

String: hotel

Originally Posted: 13 June 2012

Application ID: 1-1913-57874

Applicant Information

1. Full legal name

Fegistry, LLC

2. Address of the principal place of business

Contact Information
Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Jay Westerdal

6(b). Title

CEO

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

Jay Westerdal

7(b). Title

CEO

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 partnership

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

Washington State

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.

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

Jay Per Erik Westerdal	CEO

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

Jay Per Erik Westerdal	CEO

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

Jay Per Erik Westerdal	CEO

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

Applied-for gTLD string

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

hotel

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.

Given that .hotel is a standard five character ASCII string, we do not know of any possible issues. We have considered various unlikely scenarios, but given the fact that they have no precedent, we do not expect them to come up. We will work with our registry back-end provider, however, to ensure that no rendering or operational issues occur.

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.

Fegistry's mission for .hotel is to create a recognizable, viable, and profitable extension to bring together individuals and companies who are passionate about self-identifying themselves as in the hotel industry. There are thousands of hotels and hotel related businesses on the Internet and a registrant can create a website that identifies itself directly in the TLD. It seems fitting, as ICANN opens up an unprecedented and innovative program to expand how we use and identify with the Internet, that use cases like .hotel should be allowed as well. We are creating the opportunity for internet users to identify websites that operate in or around the hotel industry by looking just at the TLD. By owning a domain in the .hotel community it creates a win-win for most companies because they don't need to identify to the left of the dot they are a hotel related website.
It is our goal to be a financially successful company, solvent throughout our launch and profitable within our first year of operations. We believe this is an eventual reality and that our projections and financial analysis included in this application demonstrate this. We hope to grow at a rate that allows us to continually improve our registry offerings, and increase benefits for both our customers and employees. Our commitments and projections at this time are focused on conservative estimates of our revenue in order to best prepare for a TLD market with the possibility of 100,000+ TLDs in the next decade. We don't expect the demand for domains under our TLD to be big. Perhaps up to 10,000 registrations by the end of year 3, however we do have investors and a technical team that will stand behind the company if projections are higher than we anticipate.

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

i.) What is the goal of your proposed gTLD in terms of areas of specialty, service levels, or reputation?
It is our expectation that .hotel will be primarily used by companies and enthusiasts. Given the wide range of what can be classified under hotel we do not intend to limit the gTLD to a specific community. We believe that "hotel" is a internationally understood concept and word, and that the average Internet

user will understand that the content of a .hotel domain will be geared towards hotels and places users can stay.
We hope to create a community that uses the domains with respect and helps users find hotel related resources. We hope to solidify a positive and recognizable reputation as the best TLD for finding Hotel related things.

ii.) What do you anticipate your proposed gTLD will add to the current space, in terms of areas of competition, differentiation, or innovation?
Implementing .hotel into the root zone is not only necessary due to the scarcity of desirable domains in the Internet's most prominent TLDs, but further necessitated by the size and diversity of the ideas around products and services. Hotel does not fit well under any of the current gTLDs: for example, hotel is not necessarily a "commercial," "organized," "informational," or "business" endeavour. Further, given that thoughts and ideas around Hotel transcend national boundaries, it also does not fit well into the purview of ccTLDs. The .hotel TLD will provide a competitive alternative for those with the primary interest in organizing around the Hotel brand. We believe that creating a .hotel TLD will facilitate discovery of more hotels than any other current TLD.
This does not mean we expect that all of the hotel-centric sites will want to move to a .hotel extension. Many organizations and individuals may think that their current website is better served by .com, or that their non-profit hotel website is at home in .org. Consequently, by adding a .hotel to the root zone, ICANN will be improving existing TLDs by allowing them to become more focused on their intended significance, while simultaneously providing a differentiated and specific extension.

iii.) What goals does your proposed gTLD have in terms of user experience?
Fegistry believes the .hotel extension, though broadly defined by the wide spectrum of what constitutes hotel, is largely self-explanatory and its content readily apparent to both potential registrants and end-consumers. We hope that the Internet experience of both types of users will therefore be enhanced and simplified by the implementation of .hotel into the root zone. Internet users browsing and using sites with a .hotel extension will be confident that the website they are navigating will be related to hotel. We hope that this interaction between content providers and content consumers will allow the Internet's userbase to work in greater concert and to strengthen their connections globally.

iv.) Provide a complete description of the applicant's intended registration policies in support of the goals listed above.
Given that we recognize the expansiveness and diversity of what constitutes hotel, we intend to offer .hotel domains through ICANN-accredited registrars, using an open registration policy that requires no verification of any certification, training, or other quantifiable measure of merit. Additionally, it is our goal to remain in compliance with typical registration policies used by the domain name industry. Through targeted marketing efforts and niche pricing levels, we expect to see that a large majority of the domains registered will be by those with plans to develop sites related to hotels. Companies that wish to be identified as in the hotel industry may want to operate a .hotel domain in a dedicated way.

We will fully implement the requirements made by the ICANN Board with regards to the Trademark Clearinghouse, the URS, Trademark PDDRP, the RRDRP, and the UDRP. We believe the these measures have been suitably developed to prevent defensive registrations, bad faith registrations, and other malicious registrations.

v.) Will your proposed gTLD impose any measures for protecting the privacy or confidential information of registrants or users? If so, please describe any such measures.

As per the current requirements in Section 4 of the Registry Agreement, we will

implement all necessary thick WHOIS services. We recognize how imperative it is for each registry and ICANN-accredited registrar to be in full compliance with ICANN's current WHOIS standards, and we plan to update our policy in accordance with any future measures taken by the ICANN Board in regard to the continuous work by the GNSO's WHOIS Task Force and other recommendations from the SOs. We have no plans to implement any privacy or confidential measures other than fully implementing any and all such measures required by ICANN.

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

i. How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come/first-serve basis?

During our sunrise and landrush periods, which we anticipate to begin 4 months after the signing of the registry agreement and lasting for a period of some 2 months each, we will accept applications for second-level domains. Following standard procedure, the sunrise period will be reserved for those entities with appropriate IP and Trademark claims, while the landrush will be open to the public. At the conclusion of each period we will hold closed auctions for the domains that have been applied for by more than one party.

For general availability of the .hotel TLD, following the sunrise and landrush periods, we will be operating on a first-come, first-served basis. However, we reserve the right to create a list of domain names within our .hotel TLD to be set aside and then sold or auctioned off to interested parties, which we have included in the revenue for the second year of operations.

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

We have no plans to implement any cost benefits for registrants at this time. However, we have discussed the possibility of promotions, such as bulk registration discounts and advantageous pricings, should they be necessitated due to currently unforeseen circumstances or become part of a targeted marketing campaign during any part of our launch.

iii.) Note that the Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than ten years. Additionally, the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation? If so, please describe your plans.

Price increases may be necessary due to inflation or other unforeseen circumstances. However, we recognize that it is important to protect registrants from unreasonable price increases, and therefore plan not to exceed the industry-precedented reasonable maximum annual wholesale price increase of 10%, and to give written notice of at least 90 days to our registrants of such increases. We do not anticipate the need for significant price increases and are equally likely to lower the price in the future. We have no plans at this time to make further contractual commitments to our registrants regarding wholesale price escalation, but do intend to follow the best practices set forth by the industry and treat our registrants with respect, both financially and otherwise.

We intend to fully comply with the provisions in the Registry Agreement stating that registration being made available by our registrars for a period of one to ten years, while not exceeding ten years.

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.

Fegistry has considered the relevant provisions of the new TLD Registries Agreement, the GAC Advice "GAC Principles Regarding new TLDs" and the procedures adopted by other gTLD registries and intends to use the procedure described below with regards to protection of geographic names in our Registry. Prior to its launch Fegistry will compile a list of country and territory names that are subject to reservation on the second level.
Pursuant to the specification provided in ICANN's Applicant Guidebook, the list will include country and territory names based on the following internationally recognized lists:
- The short form (in English) of all country and territory names contained on the ISO 3166-1 list;
- 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
- 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;
As the above documents get updated from time to time, the exact list of reserved names will be compiled shortly before the TLD launch to account for any updates. The list of reserved names will be published on the Registry website.

Registry Services

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

Applicant has chosen CentralNic as the registry infrastructure provider for the TLD. Please see Appendix 23.1 for the acceptance letter from CentralNic. Any information regarding technical and operational capability of the proposed the TLD registry (answers to questions 23 - 44) therefore refers to CentralNic's registry infrastructure systems.
Applicant and CentralNic hereby explicitly confirm that all registry services stated below are engineered and will be provided in a manner compliant with the new gTLD Registry Agreement, ICANN consensus policies (such as Inter-Registrar Transfer Policy and AGP Limits Policy) and applicable technical standards.
Except for the registry services described above, no other services will be provided by the Registry that relate to (i) receipt of data from registrars concerning registrations of domain names and name servers; (ii) provision to registrars of status information relating to the zone servers for the TLD;(iii) dissemination of TLD zone files; (iv) operation of the Registry zone servers;

or (v) dissemination of contact and other information concerning domain name server registrations in the TLD as required by the Registry Agreement.
There are no other products or services, except those described above that the Registry Operator will provide (i) because of the establishment of a Consensus Policy, or (ii) by reason of Applicant being designated as the Registry Operator.
Any changes to the registry services that may be required at a later time in the course of the Applicant operating the registry will be addressed using rules and procedures established by ICANN such as the Registry Services Evaluation Policy.
Applicant proposes to operate the following registry services, utilising CentralNic's registry system:

23.1. Receipt of Data From Registrars
CentralNic will operate a Shared Registry System (SRS) for the TLD. The SRS consists of a database of registered domain names, host objects and contact objects, accessed via an Extensible Provisioning Protocol (EPP) interface, and a web based Registrar Console. Registrars will uses these interfaces to provide registration data to the registry.
The SRS will be hosted at CentralNic's primary operations centre in London, UK. The primary operations centre comprises a resilient, fault-tolerant network infrastructure with multiple high quality redundant links to backbone Internet carriers. The primary operations centre is hosted in Level 3's flagship European data centre and boasts significant physical security capabilities, including 24x7 patrols, CCTV and card-based access controls.
CentralNic's existing SRS system currently supports more than 250,000 domain names managed by over one 1,500 registrars. CentralNic has effective and efficient 24x7 customer support capabilities to support these domain names and registrars, and this capability will be expanded to meet the requirements of the TLD and provide additional capacity during periods of elevated activity (such as during Sunrise periods).
The SRS and EPP systems are described more fully in §24 and §25. The Registrar Console is described in §31.
EPP is an extensible protocol by definition. Certain extensions have been put in place to comply with the new gTLD registry agreement, ICANN Consensus Policies and technical standards:
1. Registry Grace Period Mapping - compliant with RFC 3915
2. DNSSEC Security Extensions - compliant with RFC 5910
3. Launch Phase Extension - will be only active during the Sunrise phase, before the SRS opens for the general public. The extension is compliant with the current Internet Draft https://github.com/wil/EPP-Launch-Phase-Extension-Specification/blob/master/draft-tan-epp-launchphase.txt
More information on EPP extensions is provided in §25.
The SRS will implement and support all ICANN Consensus Policies and Temporary Policies, including:
Uniform Domain Name Dispute Resolution Policy
Inter-Registrar Transfer Policy
Whois Marketing Restriction Policy
Restored Names Accuracy Policy
Expired Domain Deletion Policy
AGP Limits Policy

23.2. Provision to Registrars of Status Information Relating to the Zone Servers
CentralNic will operate a communications channel to notify registrars of all operational issues and activity relating to the DNS servers which are authoritative for the TLD. This includes notifications relating to:
1. Planned and unplanned maintenance;
2. Denial-of-service attacks;
3. unplanned network outages;
4. delays in publication of DNS zone updates;
5. security incidents such as attempted or successful breaches of access controls;
6. significant changes in DNS server behaviour or features;

7. DNSSEC key rollovers.
Notifications will be sent via email (to preregistered contact addresses), with additional notifications made via an off-site maintenance site and via social media channels.

23.3. Dissemination of TLD Zone Files
CentralNic will make TLD zone files available via the Centralized Zone Data Access Provider according to specification 4, section 2 of the Registry Agreement.
Applicant will enter into an agreement with any Internet user that will allow such user to access an Internet host server or servers designated by Applicant and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider (the "CZDA Provider"). Applicant will provide access to zone file data using the file format described in Section 2.1.4 of Specification 4 of the New gTLD Registry Agreement.
Applicant, 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 the Internet host machine name and IP address.
Applicant will provide the Zone File FTP (or other Registry supported) service for an ICANN-specified and managed URL for the user to access the Registry's zone data archives. Applicant will grant the user a non-exclusive, non-transferable, limited right to access Applicant's Zone File FTP 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.
Applicant will provide zone files using a sub-format 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.
Applicant, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months. Applicant will allow users to renew their Grant of Access.
Applicant will provide, and CZDA Provider will facilitate, access to the zone file to user at no cost.

23.4. Operation of the Registry Zone Servers
The TLD zone will be served from CentralNic's authoritative DNS system. This system has operated at 100% service availability since 1996 and has been developed into a secure and stable platform for domain resolution. Partnering with Community DNS, CentralNic's DNS system includes nameservers in more than forty cities, on five continents. The DNS system fully complies with all relevant RFCs and all ICANN specifications, and has been engineered to ensure resilience and stability in the face of denial-of-service attacks, with substantial overhead and geographical dispersion.
The DNS system is described further in §35.

23.5. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations
CentralNic will operate a Whois service for the TLD. The Whois service will provide information about domain names, contact objects, and name server objects stored in the Shared Registry System via a port-43 service compliant with RFC 3912. The Whois service will permit interested parties to obtain information about the Registered Name Holder, Administrative, Technical and Billing contacts for domain names. The Whois service will return records in a standardised format which complies with ICANN specifications.
CentralNic will provide access to the Whois service at no cost to the general public.
CentralNic's Whois service supports a number of features, including rate limiting to prevent abuse, privacy protections for natural persons, and a secure Searchable Whois Service. The Whois service is more fully described in §26.
Should ICANN specify alternative formats and protocols for the dissemination of

Domain Name Registration Data, CentralNic will implement such alternative specifications as soon as reasonably practicable.

23.6. DNSSEC
The TLD zone will be signed by DNSSEC. CentralNic uses the award-winning signer technology from Xelerance Corporation. Zone files will be signed using NSEC3 with opt-out, following a DNSSEC Practice Statement detailed in §43. CentralNic's DNSSEC implementation complies with RFCs 4033, 4034, 4035, 4509 and follows the best practices described in RFC 4641. Hashed Authenticated Denial of Existence (NSEC3) will be implemented, which complies with RFC 5155. The SRS will accept public-key material from child domain names in a secure manner according to industry best practices (specifically the secDNS EPP extension, described in RFC 5910). CentralNic will 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. CentralNic will publish its DPS following the format described in the "DPS-framework" Internet Draft within 180 days after that draft becomes an RFC.

23.7. Rights Protection Mechanisms
Applicant will provide all mandatory Rights Protection Mechanisms that are specified in the Applicant Guidebook (version 11 January 2012), namely Trademark Claims Service (section 6.1) and Sunrise service (section 6.2). All the required RPM-related policies and procedures such as UDRP, URS, PDDRP and RRDRP will be adopted and used in the TLD. More information is available in §29.
In addition to such RPMs, Applicant may develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party's legal rights. Applicant will include all ICANN mandated and independently developed RPMs in the registry-registrar agreement entered into by ICANN-accredited registrars authorised to register names in the TLD. Applicant shall implement these mechanisms in accordance with requirements established by ICANN each of the mandatory RPMs set forth in the Trademark Clearinghouse.
The "LaunchPhase" EPP extension (described above) will be used to implement an SRS interface during the Sunrise period for the TLD. Depending on the final specification for the Trademark Claims Service (details of which have not yet been published), an additional EPP extension may be required in order to implement this service. If this is necessary, the extension will be designed to minimise its effect on the operation of the SRS and the requirements on registrars, and will only be in place for a limited period while the Trademark Claims Service is in effect for the TLD.

23.8. Registrar Support and Account Management
CentralNic will leverage its 16 years of experience of supporting over 1,500 registrars to provide high-quality 24x7 support and account management for the TLD registrars. CentralNic's experienced technical and customer support personnel will assist the TLD registrars during the on-boarding and OT&E process, and provide responsive personal support via email, phone and a web based support ticketing system.

23.9. Reporting to ICANN
Applicant and CentralNic will compile and transmit a monthly report to ICANN relating to the TLD. This report will comply with Specification 3 of the New gTLD Registry Agreement.

23.10. Personnel Resources of CentralNic
The technical, operations and support functions of the registry will performed in-house by CentralNic's personnel. These personnel perform these functions on a full-time basis.

23.10.1. Technical Operations
Technical Operations refers to the deployment, maintenance, monitoring and security of the registry system, including the SRS and the other critical

registry functions. Technical Operations staff design, build, deploy and maintain the technical infrastructure that supports the registry system, including power distribution, network design, access control, monitoring and logging services, and server and database administration. Internal helpdesk and incident reporting is also performed by the Technical Operations team. The Technical Operations team performs 24x7 monitoring and support for the registry system and mans the Network Operations Centre (NOC) from which all technical activities are co-ordinated.
CentralNic intends to maintain a Technical Operations team consisting of the following positions. These persons will be responsible for managing, developing and monitoring the registry system for the TLD on a 24x7 basis:
Senior Operations Engineer(s)
Operations Engineer(s)
Security Engineer

23.10.2. Technical Development
The Technical Development team develops and maintains the software which implements the critical registry functions, including the EPP, Whois, Zone file generation, data escrow, reporting, backoffice and web-based management systems (intranet and extranet), and open-source registrar toolkit software. All critical registry software has been developed and maintained in-house by this team.
CentralNic intends to maintain a Technical Development team consisting of the following positions. These persons will be responsible for maintaining and developing the registry software which will support the TLD:
Senior Technical Developer x 2
Technical Developer x 3

23.10.3. Technical Support
Technical Support refers to 1st, 2nd and 3rd line support for registrars and end-users. Areas covered include technical support for systems and services, billing and account management. Support personnel also deal with compliance and legal issues such as UDRP and URS proceedings, abuse reports and enquiries from law enforcement.
1st line support issues are normally dealt with by these personnel. 2bd and 3rd line support issues (relating to functional or operational issues with the registry system) are escalated to Technical Operations or Technical Development as necessary.
The Technical Support team will consist of the following positions:
Operations Manager
Support Manager
Support Agent(s)
Our overseas account managers also perform basic support functions, escalating to the support agents in London where necessary.

23.10.4. Key Personnel

23.10.4.1. Gavin Brown - Chief Technology Officer
Gavin has worked at CentralNic since 2001, becoming CTO in 2005. He has overall responsibility for all aspects of the SRS, Whois, DNS and DNSSEC systems. He is a respected figure in the domain industry and has been published in several professional technical journals, and co-authored a book on the Perl programming language. He also participates in a number of technical, public policy and advocacy groups and several open source projects. Gavin has a BSc (hons) in Physics from the University of Kent.

23.10.4.2. Jenny White - Operations Manager
Jenny has been with CentralNic for nine years. Throughout this time she has expertly managed customer relations with external partners, prepared new domain launch processes and documentation, managed daily support and maintenance for over 1,500 Registrars, carried out extensive troubleshooting within the registrar environment to ensure optimum usability for registrars across communication platforms, handled domain disputes (from mediation to WIPO filing), and liaised with WIPO to implement changes to the Dispute Resolution

Procedure when necessary.

23.10.4.3. Adam Armstrong - Senior Operations Engineer
Adam has recently joined CentralNic as Senior Operations Engineer. In this role he is responsible for the operation and development of the system and network infrastructure for the registry system. Adam has previously worked at a number of large UK ISPs including Jersey Telecom and Packet Exchange. He is also the lead developer of Observium, a network management system used by ICANN (amongst others). Adam has brought his strong knowledge of network design, management and security to bear at CentralNic and will oversee the operation of the SRS for the TLD.

23.10.4.4. Milos Negovanovic - Senior Technical Developer
Milos has worked at CentralNic since 2009. He has a background in building rich web applications and protocol servers. His main areas of responsibility are the Registrar Console, EPP and backoffice functions.

23.10.4.5. Mary O'Flaherty - Senior Technical Developer
Mary has worked at CentralNic since 2008. She plays an integral role in the ongoing design, development and maintenance of the registry as a whole and has specific experience with the EPP system, Registrar Console and Staff Console. Mary has a 1st class Honors degree in Computer Science from University College Cork and has previously worked for Intel and QAD Ireland.

23.10.5. Job Descriptions
CentralNic will recruit a number of new employees to perform technical duties in relation to the TLD and other gTLDs. The following job descriptions will be used to define these roles and select candidates with suitable skills and experience.

23.10.5.1. Operations Engineer
Operations Engineers assist in the maintenance and development of the network and server infrastructure of the registry system. Operations Engineers have a good knowledge of the TCP/IP protocol stack and related technologies, and are familiar with best practice in the areas of network design and management and system administration. They should be competent system administrators with a good knowledge of Unix system administration, and some knowledge of shell scripting, software development and databases. Operations Engineers have 1-2 year's relevant commercial experience. Operations Engineers report to and work with the Senior Operations Engineer, who provides advice and mentoring. Operations Engineers participate in manning the NOC on a 24x7 basis and participate in the on-call shift rota.

23.10.5.2. Security Engineer
Security Engineers enhance and assure the security of the registry system. Day-to-day responsibilities are: responding to security incidents, performing analysis and remediating vulnerabilities, conducting tests of access controls, refining system configuration to improve security, training other team members, reviewing source code, maintaining security policies and procedures, and gathering intelligence relating to threats to the registry. Security Engineers have 1-2 year's relevant commercial experience. This role reports to and works with the Senior Operations Engineer and CTO. Security Engineers participate in manning the NOC on a 24x7 basis and participate in the on-call shift rota.

23.10.5.3. Technical Developer
Technical Developers are maintain the software which supports the registry. Day-to-day responsibilities are developing new systems in response to requests from management and customers, correcting bugs in existing software, and improving its performance. Technical Developers have a good knowledge of general programming practices including use of revision control and code review systems. Developers have a good awareness of security issues, such as those described in advisories published by the oWASP Project. Developers have at least one years' commercial experience in developing applications in programming languages such as PHP, Perl, and Python, although knowledge of

domain technologies such as EPP and DNS is not critical. Technical Developers work as part of a team, with advice and mentoring from the Senior Technical Developers, to whom they report.

23.10.6. Resource Matrix
To provide a means to accurately and objectively predict human resource requirements for the operation of the registry system, CentralNic has developed a Resourcing Matrix, which assigns a proportion of each employee's available time to each aspect of registry activities. These activities include technical work such as operations and development, as well as technical support, registrar account management, rights protection, abuse prevention, and financial activity such as payroll, cash collection, etc. This matrix then permits the calculation of the total HR resource assigned to each area.
A copy of the Resourcing Matrix is included as Appendix 23.2. It is important to note that the available resources cover the operation of CentralNic's entire registry operations: this includes CentralNic's own domain registry portfolio (uk.com, us.com, etc), the .LA ccTLD, as well as the gTLDs which CentralNic will provides registry service for.
The actual proportion of human technical resources required specifically for the TLD is determined by the relative size of the TLD to the rest of CentralNic's operations. This calculation is based on the projected number of domains after three years of operation: the optimistic scenario is used to ensure that sufficient personnel is on hand to meet periods of enhanced demand. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Since the optimistic projection for the number of domains registered in the TLD after three years is 10,000, the TLD will therefore require 0.22% of CentralNic's total available HR resources in order operate fully and correctly. In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
24.1. Registry Type
CentralNic operates a "thick" registry in which the registry maintains copies of all information associated with registered domains. Registrars maintain their own copies of registration information, thus registry-registrar synchronization is required to ensure that both registry and registrar have consistent views of the technical and contact information associated with registered domains. The Extensible Provisioning Protocol (EPP) adopted supports the thick registry model. See §25 for further details.

24.2. Architecture
Figure 24.1 provides a diagram of the overall configuration of the SRS. This diagram should be viewed in the context of the overall architecture of the registry system described in §32.
The SRS is hosted at CentralNic's primary operations centre in London. It is is connected to the public Internet via two upstream connections, one of which is

provided by Qube. Figure 32.1 provides a diagram of the outbound network connectivity. Interconnection with upstream transit providers is via two BGP routers which connect to the firewalls which implement access controls over registry services.
Within the firewall boundary, connectivity is provided to servers by means of resilient gigabit ethernet switches implementing Spanning Tree Protocol.
The registry system implements two interfaces to the SRS: the standard EPP system (described in §25) and the Registrar Console (described in §31). These systems interact with the primary registry database (described in §33). The database is the central repository of all registry data. Other registry services also interact with this database.
An internal "Staff Console" is used by CentralNic personnel to perform management of the registry system.

24.3. EPP System Architecture
A description of the characteristics of the EPP system is provided in §25. This response describes the infrastructure which supports the EPP system.
A network diagram for the EPP system is provided in Figure 24.2. The EPP system is hosted at the primary operations centre in London. During failover conditions, the EPP system operates from the Isle of Man Disaster Recovery site (see §34).
CentralNic's EPP system has a three-layer logical and physical architecture, consisting of load balancers, a cluster of front-end protocol servers, and a pool of application servers. Each layer can be scaled horizontally in order to meet demand.
Registars establish TLS-secured TCP connections to the load balancers on TCP port 700. Load is balanced using DNS round-robin load balancing.
The load balancers pass sessions to the EPP protocol servers. Load is distributed using a weighted-least-connections algorithm. The protocol servers run the Apache web server with the mod_epp and mod_proxy_balancer modules. These servers process session commands ("hello", "login" and "logout") and function as reverse proxies for query and transform commands, converting them into plain HTTP requests which are then distributed to the application servers. EPP commands are distributed using a weighted-least-connections algorithm. Application servers receives EPP commands as plain HTTP requests, which are handled using application business logic. Application servers process commands and prepare responses which are sent back to the protocol servers, which return responses to clients over EPP sessions.
Each component of the system is resilient: multiple inbound connections, redundant power, high availability firewalls, load balancers and application server clusters enable seamless operation in the event of component failure. This architecture also allows for arbitrary horizontal scaling: commodity hardware is used throughout the system and can be rapidly added to the system, without disruption, to meet an unexpected growth in demand.
The EPP system will comprise of the following systems:
4x load balancers (1U rack mount servers with quad-core Intel processors, 16GB RAM, 40GB solid-state disk drives, running the CentOS operating system using the Linux Virtual Server [see http://www.linuxvirtualserver.org/])
8x EPP protocol servers (1U rack mount servers with dual-core Intel processors, 16GB RAM, running the CentOS operating system using Apache and mod_epp)
20x application servers (1U rack mount servers with dual-core Intel processors, 4GB of RAM, running the CentOS operating system using Apache and PHP)

24.3.1. mod_epp
mod_epp is an Apache server module which adds support for the EPP transport protocol to Apache. This permits implementation of an EPP server using the various features of Apache, including CGI scripts and other dynamic request handlers, reverse proxies, and even static files. mod_epp was originally developed by Nic.at, the Austrian ccTLD registry. Since its release, a large number of ccTLD and other registries have deployed it and continue to support its development and maintenance. Further information can be found at http://sourceforge.net/projects/aepps. CentralNic uses mod_epp to manage EPP sessions with registrar clients, and to convert EPP commands into HTTP requests which can then be handled by backend application servers.

24.3.2. mod_proxy_balancer
mod_proxy_balancer is a core Apache module. Combined with the mod_proxy module, it implements a load-balancing reverse proxy, and includes a number of load balancing algorithms and automated failover between members of a cluster. CentralNic uses mod_proxy_balancer to distribute EPP commands to backend application servers.

24.4. Performance
CentralNic performs continuous remote monitoring of its EPP system, and this monitoring includes measuring the performance of various parts of the system. As of writing, the average round-trip times (RTTs) for various functions of the EPP system were as follows:
connect time: 87ms
login time: 75ms
hello time: 21ms
check time: 123ms
logout time: 20ms
These figures include an approximate latency of 2.4ms due to the distant between the monitoring site and the EPP system. They were recorded during normal weekday operations during the busiest time of the day (around 1300hrs UTC) and compare very favourably to the requirement of 4,000ms for session commands and 2,000ms for query commands defined in the new gTLD Service Level Agreement. RTTs for overseas registrars will be higher than this due to the greater distances involved, but will remain well within requirements.

24.5. Scaling
Horizontal scaling is preferred over vertical scaling. Horizontal scaling refers to the introduction of additional nodes into a cluster, while vertical scaling involves using more powerful equipment (more CPU cores, RAM etc) in a single system. Horizontal scaling also encourages effective mechanisms to ensure high-availability, and eliminate single points of failure in the system. Vertical scaling leverages Moore's Law: when units are depreciated and replaced, the new equipment is likely to be significantly more powerful. If the average lifespan of a server in the system is three years, then its replacement is likely to be around four times as powerful as the old server.
For further information about Capacity Management and Scaling, please see §32.

24.6. Registrar Console
The Registrar Console is a web-based registrar account management tool. It provides a secure and easy-to-use graphical interface to the SRS. It is hosted on a virtual platform at the primary operations centre in London. As with the rest of the registry system, during a failover condition it is operated from the Isle of Man. The virtual platform is described in Figure 24.3.
The features of the Registrar Console are described in §31.
The virtual platform is a utility platform which supports systems and services which do not operate at significant levels of load, and which therefore do not require multiple servers or the additional performance that running on "bare metal" would provide. The platform functions as a private cloud, with redundant storage and failover between hosts.
The Registrar Console currently sustains an average of 6 page requests per minute during normal operations, with peak volumes of around 8 requests per minute. Volumes during weekends are significantly lower (fewer than 1 requests per minute). Additional load resulting from this and other new gTLDs is expected to result in a trivial increase in Registrar Console request volumes, and CentralNic does not expect additional hardware resources to be required to support it.

24.7. Quality Assurance
CentralNic employs the following quality assurance (QA) methods:
1. 24x7x365 monitoring provides reports of incidents to NOC
2. Quarterly review of capacity, performance and reliability
3. Monthly reviews of uptime, latency and bandwidth consumption
4. Hardware depreciation schedules

5. Unit testing framework
6. Frequent reviews by QA working group
7. Schema validation and similar technologies to monitor compliance on a real-time, ongoing basis
8. Revision control software with online annotation and change logs
9. Bug Tracking system to which all employees have access
10. Code Review Policy in place to enforce peer review of all changes to core code prior to deployment
11. Software incorporates built-in error reporting mechanisms to detect flaws and report to Operations team
12. Four stage deployment strategy: development environment, staging for internal testing, OT&E deployment for registrar testing, then finally production deployment
13. Evidence-based project scheduling
14. Specification development and revision
15. Weekly milestones for developers
16. Gantt charts and critical path analysis for project planning

Registry system updates are performed on an ongoing basis, with any user-facing updates (ie changes to the behaviour of the EPP interface) being scheduled at specific times. Disruptive maintenance is scheduled for periods during which activity is lowest.

24.8. Billing

CentralNic operates a complex billing system for domain name registry services to ensure registry billing and collection services are feature rich, accurate, secure, and accessible to all registrars. The goal of the system is to maintain the integrity of data and create reports which are accurate, accessible, secured, and scalable. The foundation of the process is debit accounts established for each registrar. CentralNic will withdraw all domain fees from the registrar's account on a per-transaction basis. CentralNic will provide fee-incurring services (e.g., domain registrations, registrar transfers, domain renewals) to a registrar for as long as that registrar's account shows a positive balance.

Once ICANN notifies Applicant that a registrar has been issued accreditation, CentralNic will begin the registrar on-boarding process, including setting up the registrar's financial account within the SRS.

24.9. Registrar Support

CentralNic provides a multi-tier support system on a 24x7 basis with the following support levels:

1st Level: initial support level responsible for basic customer issues. The first job of 1st Level personnel is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem.

2nd Level: more in-depth technical support level than 1st Level support containing experienced and more knowledgeable personnel on a particular product or service. Technicians at this level are responsible for assisting 1st Level personnel solve basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues.

3rd Level: the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced problems. Level 3 personnel are experts in their fields and are responsible for not only assisting both 1st and 2nd level personnel, but with the research and development of solutions to new or unknown issues.

CentralNic provides a support ticketing system for tracking routine support issues. This is a web based system (available via the Registrar Console) allowing registrars to report new issues, follow up on previously raised tickets, and read responses from CentralNic support personnel.

When a new trouble ticket is submitted, it is assigned a unique ID and priority. The following priority levels are used:

1. Normal: general enquiry, usage question, or feature enhancement request. Handled by 1st level support.
2. Elevated: issue with a non-critical feature for which a work-around may or

may not exist. Handled by 1st level support.
3. Severe: serious issue with a primary feature necessary for daily operations for which no work-around has been discovered and which completely prevents the feature from being used. Handled by 2nd level support.
4. Critical: A major production system is down or severely impacted. These issues are catastrophic outages that affect the overall Registry System operations. Handled by 3rd level support.
Depending on priority, different personnel will be alerted to the existence of the ticket. For example, a Priority 1 ticket will cause a notification to be emailed to the registrar customer support team, but a Priority 4 ticket will result in a broadcast message sent to the pagers of senior operations staff including the CTO. The system permits escalation of issues that are not resolved within target resolution times.

24.10. Enforcement of Eligibility Requirements
The SRS supports enforcement of eligibility requirements, as required by specific TLD policies.
Figure 24.4 describes the process by which registration requests are validated. Prior to registration, the registrant's eligibility is validated by a Validation Agent. The registrant then instructs their registrar to register the domain. The SRS returns an "Object Pending" result code (1001) to the registrar.
The request is sent to the Validation Agent by the registry. The Validation Agent either approves or rejects the request, having reconciled the registration information with that recorded during the eligibility validation. If the request has been approved, the domain is fully registered. If it is rejected, the domain is immediately removed from the database. A message is sent to the registrar via the EPP message queue in either case. The registrar then notifies the registrant of the result.

24.11. Interconnectivity With Other Registry Systems
The registry system is based on multiple resilient stateless modules. The SRS, Whois, DNS and other systems do not directly interact with each other. Interactions are mediated by the database which is the single authoritative source of data for the registry as a whole. Individuals modules perform "CRUD" (create, read, update, delete) actions upon the database. These actions then affect the behaviour of other registry systems: for example, when a registrar adds the "clientHold" status to a domain object, this is recorded in the database. When a query is received for this domain via the Whois service, the presence of this status code in the database results in the "Status: CLIENT HOLD" appearing in the whois record. It will also be noted by the zone generation system, resulting in the temporary removal of the delegation of the domain name from the DNS.

24.12. Resilience
The SRS has a stateless architecture designed to be fully resilient in order to provide an uninterrupted service in the face of failure or one or more parts of the system. This is achieved by use of redundant hardware and network connections, and by use of continuous "heartbeat" monitoring allowing dynamic and high-speed failover from active to standby components, or between nodes in an active-active cluster. These technologies also permit rapid scaling of the system to meet short-term increases in demand during "surge" periods, such as during the initial launch of a new TLD.

24.12.1. Synchronisation Between Servers and Sites
CentralNic's system is implemented as multiple stateless systems which interact via a central registry database. As a result, there are only a few situations where synchronisation of data between servers is necessary:
1. replication of data between active and standby servers (see §33). CentralNic implements redundancy in its database system by means of an active⁄standby database cluster. The database system used by CentralNic supports native real-time replication of data allowing operation of a reliable hot standby server. Automated heartbeat monitoring and failover is implemented to ensure continued access to the database following a failure of the primary database system.

2. replication is used to synchronise the primary operations centre with the Disaster Recovery site hosted in the Isle of Man (see §34). Database updates are replicated to the DR site in real-time via a secured VPN, providing a "hot" backup site which can be used to provide registry services in the event of a failure at the primary site.

24.13. Operational Testing and Evaluation (OT&E)
An Operational Testing and Evaluation (OT&E) environment is provided for registrars to develop and test their systems. The OT&E system replicates the SRS in a clean-room environment. Access to the OT&E system is unrestricted and unlimited: registrars can freely create multiple OT&E accounts via the Registrar Console.

24.14. Resourcing
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to more than one full-time post. CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require 0.22% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

25. Extensible Provisioning Protocol (EPP)

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
The Extensible Provisioning Protocol (EPP) is an application layer client-server protocol for the provisioning and management of objects stored in a shared central repository. EPP defines generic object management operations and an extensible framework that maps protocol operations to objects. EPP has become established as the common protocol by which domain registrars can manage domains, nameservers and contact details held by domain registries. It is widely deployed in the gTLD and ccTLD registry space.
CentralNic has operated its EPP system since 2005, and it currently operates at significant load in terms of registrars, sessions and transaction volumes.
CentralNic's EPP system is fully compliant with the following RFC specifications:
5730 - Base Protocol
5731 - domains

5732 - Host Objects
5733 - Contact Objects
5734 - TCP Transport
3735 - Extension Guidelines
3915 - RGP Extension
5910 - DNSSEC Extension

25.1. Description of Interface
EPP is a stateful XML protocol layered over TCP (see RFC 3734). Protected using lower-layer security protocols, clients exchange identification, authentication, and option information, and engage in a series of client-initiated command-response exchanges. All EPP commands are atomic (there is no partial success or partial failure) and designed so that they can be made idempotent (executing a command more than once has the same net effect on system state as successfully executing the command once).
EPP provides four basic service elements: service discovery, commands, responses, and an extension framework that supports definition of managed objects and the relationship of protocol requests and responses to those objects.
EPP servers respond to client-initiated communication (which can be either a lower-layer connection request or an EPP service discovery message) by returning a greeting to a client. The server then responds to each EPP command with a coordinated response that describes the results of processing the command.
EPP commands fall into three categories: session management, queries, and transform commands. Session management commands are used to establish and end persistent sessions with an EPP server. Query commands perform read-only object information retrieval operations. Transform commands perform read-write object management operations.
Commands are processed by a server in the order they are received from a client. The protocol includes features that allow for offline review of transform commands before the requested action is completed. In such situations, the response clearly notes that the command has been received but that the requested action is pending. The corresponding object then reflects processing of the pending action. The server will also notify the client when offline processing of the action has been completed. Object mappings describe standard formats for notices that describe completion of offline processing.
EPP uses XML namespaces to provide an extensible object management framework and to identify schemas required for XML instance parsing and validation. These namespaces and schema definitions are used to identify both the base protocol schema and the schemas for managed objects.

25.1.1. Objects supported
Registrars may create and manage the following object types in the CentralNic EPP system:
domains (RFC 5731)
host objects (RFC 5732)
contact objects (RFC 5733)

25.1.2. Commands supported
CentralNic supports the following EPP commands:
"hello" - retrieve the "greeting" from the server
"login" and "logout" - session management
"poll" - message queue management
"check" - availability check
"info" - object information
"create" - create object
"update" - update object
"renew" - renew object
"delete" - delete object
"transfer" - manage object transfer

25.2. EPP state diagram
Figure 25.1 describes the state machine for the EPP system. Clients establish a

connection with the server, which sends a greeting. Clients then authenticate, and once a login session is established, submits commands and receive responses until the server closes the connection, the client sends a logout command, or a timeout is reached.

25.3. EPP Object Policies
The following policies apply to objects provisioned via the EPP system:

25.3.1. domains
1. domains must comply with the syntax described in RFC 1035 §2.3.1. Additionally, the first label of the name must be between 3 and 63 characters in length.
2. domains must have a registrant attribute which is associated with a contact object in the database.
3. domains must have an administrative contact attribute which is associated with a contact object in the database.
4. domains must have a technical contact which attribute is associated with a contact object in the database.
5. domains may have an billing contact attribute which is associated with a contact object in the database.
6. domains may have between 0 (zero) and 13 DNS servers. A domain with no name servers will not resolve and no records will be published in the DNS
7. the host object model for domains is used rather than the host attribute model.
8. domains may have a number of status codes. The presence of certain status codes indicates the domain's position in the lifecycle, described further in §27.
9. where policy requires, the server may respond to a "domain:create" command with an "Object Pending" (1001) response. When this occurs, the domain is placed onto the pendingCreate status while an out-of-band validation process takes place.
10. when registered, the expiry date of a domain may be set up to ten years from the initial date of registration. Registrars can specify registration periods in one-year increments from one to ten.
11. when renewed, the expiry date of a domain may be set up to ten years from the current expiry date. Registrars can specify renewal periods in one-year increments from one to ten. domains which auto-renew are renewed for one year at a time.
12. domains must have an authInfo code which is used to authenticate inter-registrar transfer requests. This authInfo code may contain up to 48 bytes of UTF-8 character data.
13. domains may have one or more DS records associated with them. DS records are managed via the secDNS EPP extension, as specified in RFC 5910.
14. only the sponsoring registrar of the domain may submit "update", "renew" or "delete" commands for the domain.

25.3.2. Host objects
1. host names must comply with RFC 1035. The maximum length of the host name may not exceed 255 characters.
2. in-bailiwick hosts must have an IPv4 address. They may optionally have an IPv6 address.
3. multiple IP addresses are not currently permitted.
4. sponsorship of hosts is determined as follows: if an object is in-bailwick (ie child of a domain in the database, and therefore also child to a TLD in the system), then the sponsor is the sponsor of the parent domain. If the object is out-of-bailiwick, the sponsor is the registrar which created the contact.
5. if a registrar submits a change to the name of a host object, if the new host name is subordinate to an in-bailiwick domain, then that registrar must be the sponsor of the new parent domain.
6. registrars are not permitted to create hosts that are subordinate to a non-existent in-bailiwick domain, or to change the name of a host object so that it us subordinate to a non-existent in-bailiwick domain.
7. a host cannot be deleted if one or more domains are delegated to it (the registry deletes hosts to remove orphan glue, see §28).

8. inter-registrar transfers are not permitted.
9. only the sponsoring registrar of the host may submit "update" or "delete" commands for the object.

25.3.3. Contact objects
1. contact IDs may only contain characters from the set [A-Z, 0-9, . (period), - (hyphen) and - (underscore)] and are case-insensitive.
2. phone numbers and email addresses must be valid as described in RFC 5733 §2.5 and §2.6.
3. contact information is accepted and stored in "internationalized" format only: that is, contact objects only have a single "contact:postalInfo" element and the type attribute is always "int".
4. the "contact:org", "contact:sp", "contact:pc", "contact:phone" and "contact:fax" elements are optional.
5. contacts must have an authInfo code which is used in inter-registrar transfers. This code may contain up to 48 bytes of UTF-8 character data.
6. a contact cannot be deleted if one or more domains are associated with it.
7. only the sponsoring registrar of the contact may submit "update" or "delete" commands for the object.

25.4. EPP Extensions
CentralNic supports the following EPP extensions. CentralNic's implementations fully comply with the required specifications.

25.4.1. Registry Grace Period Mapping
Various grace periods and hold periods are supported by the Registry Grace Period mapping, as defined in RFC 3915. This is described further in §27.

25.4.2. DNSSEC Security Extensions Mapping
Registrars may submit Delegation Signer (DS) record information for domains under their sponsorship. This permits the establishment of a secure chain-of-trust for DNSSEC validation.
CentralNic supports the specification defined in RFC 5910. This supports two interfaces: the DS Data Interface and Key Data Interface. CentralNic supports the former interface (DS Data), where registrars submit the keytag, algorithm, digest type and digest for DS records as XML elements, rather than as key data. Key data is stored if provided as a child element of the "secDNS:dsData" element. The maxSigLife element is optional in the specification and is not currently supported.

25.4.3. Launch Phase Extension
CentralNic has assisted development of a standard EPP extension for registry "launch phases" (ie Sunrise and Landrush periods), during which the steady-state mode of "first-come, first-served" operation does not apply. This extension permits registrars to submit requests for domains with claimed rights such as a registered trademark. The extension is currently described in an Internet-Draft (see http://tools.ietf.org/html/draft-tan-epp-launchphase-00). It is hoped that this draft will eventually be published as an RFC which can be implemented by other registries and registrars.
CentralNic's system implements this extension and will support the most recent version of the draft during the initial launch of the TLD. Once the TLD enters General Availability, this extension will no longer be available for use by registrars. Example frames describing the use of this extension are included in Appendix 25.2. As of writing, the current draft does not include a full schema definition, but a schema from a previous version has been included in Appendix 25.3. When the Draft is updated to include a schema, it will be based on this version.

25.5. Registrar Credentials and Access Control
Registrars are issued with a username (their registrar ID) and a password. This password cannot be used to access any other service and only this password can be used to access the EPP system. Registrar officers with the "Management" access level can change their EPP password via the Registrar Console.
RFC 5730 requires "mutual, strong client-server authentication". CentralNic

requires that all registrars connect using an SSL certificate. This certificate may be obtained from a recognised certificate authority, or it may be a self-signed certificate registered with CentralNic via the Registrar Console. Registrar officers with the "Management" access level can upload SSL certificates for their account.

25.6. Session Limits and Transaction Volumes
There are no limits on the number of active sessions a registrar can maintain with the server. Similarly, there are no limits on the volume of transactions a registrar may send. However the system is fully capable of imposing connection limits and this measure may be used in future to ensure equal access amongst registrars.

25.7. Transaction Logging and Reporting
All "transform" commands are logged. Transform commands are: "create", "renew", "update", "delete" and "transfer". The system logs the time and date when the command was received, the registrar which submitted it, the request and response frames, the result code and message. All commands, whether successful or not, are logged.
The transaction log is stored in the primary registry database. Registrars have access to the log for their account via the Registrar Console. The log viewer permits filtering by command, object type, object ID (domain, host name, contact ID), result code and timestamp.
Query commands ("check", "info", "poll op="req"") and session commands ("login", "logout" and "hello") are not logged due to the large volume of such queries (particularly "check" queries). The EPP system uses counters for these commands to facilitate generation of monthly reports.

25.8. EPP Message Queue
The EPP protocol provides a message queue to provide registrars with notifications for out-of-band events. CentralNic currently supports the following EPP message notifications:
approved inbound transfer
rejected inbound transfer
new outbound transfer
cancelled outbound transfer
approved or rejected domain registration request (where TLD policy requires out-of-band approval of "domain:create" requests)

25.9. Registrar Support, Software Toolkit
CentralNic has supported EPP for many years. CentralNic has released a number of open source client libraries for several popular programming languages. These are used by registrars and registries around the world. CentralNic maintains the following open source EPP libraries:
Net::EPP, a general purpose EPP library for Perl. See http://code.google.com/p/perl-net-epp/
Preppi, a graphical EPP client written in Perl. See https://www.centralnic.com/company/labs/preppi
Net_EPP, a PHP client class for EPP. See https://github.com/centralnic/php-epp
Simpleepp, a Python client class for EPP. See https://bitbucket.org/milosn/simpleepp
tx-epp-proxy, a EPP reverse proxy for shared-nothing client architectures written in Python. See https://bitbucket.org/milosn/tx-epp-proxy
These libraries are available for anyone to use, at no cost. CentralNic develops these libraries, and accepts submissions and bug reports from users around the world.

25.10. Quality Assurance, RFC Compliance
To ensure that its EPP system fully complies with the relevant specifications documents, CentralNic has implemented the following:

25.10.1. Schema Validation
The EPP system automatically validates all response frames against the XSD schema definitions provided in the RFCs. Should a non-validating response be

sent to a registrar, an alert is raised with the NOC to be investigated and corrected. By default, this feature is disabled in the production environment but it is enabled in all other environments (as described below).

25.10.2. Multi-stage Deployment and Testing
EPP system code is developed, tested and deployed in a multi-stage environment:
1. Developers maintain their own development environment in which new code is written and changes are prepared. Development environments are configured with the highest level of debugging and strictness to provide early detection of faults.
2. All changes to the EPP system are subjected to peer review: other developers in the team must review, test and sign off the changes before being committed (or, if developed on a branch, being merged into the stable branch).
3. Changes to EPP system code are then deployed in the OT&E environment. Registrars continually test this system as part of their own QA processes, and this additional phase provides an additional level of quality assurance.

25.10.3. Registrar Feedback
Registrars are provided with an easy way to report issues with the EPP system, and many perform schema validation on the responses they receive. When issues are detected by registrars, they are encouraged to submit bug reports so that developers can rectify the issues.

25.11. EPP System Resourcing
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to more than one full-time person.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require 0.22% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

26. Whois

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
Whois is one of the oldest Internet protocols still in use. It allows interested persons to retrieve information relating to Internet resources

(domain names and IP addresses). Whois services are operated by the registries of these resources, namely TLD registries and RIRs.
Whois is described by RFC 3912, which serves as a description of existing systems rather than requiring specific behaviours from clients and servers. The protocol is a query-response protocol, in which both the query and the response are opaque to the protocol, and their meanings are known only the server and to the human user who submits a query. Whois has a number of limitations, but remains ubiquitous as a means for obtaining information about name and number resources.

26.1. Compliance
The Whois service for the TLD will comply with RFC3912 and Specifications 4 and 10 of the New gTLD Registry Agreement. The service will be provided to the general public at no cost. If ICANN specify alternative formats and protocols (such as WEIRDS) then CentralNic will implement these as soon as reasonably practicable.
CentralNic will monitor its Whois system to confirm compliance. Monitoring stations will check the behaviour and response of the Whois service to ensure the correctness of Whois records. CentralNic will maintain a public Whois contact to which bug reports and other questions about the Whois service can be directed.

26.2. Domain Name
By default, any query is assumed to be a domain name unless a keyword is prepended to the query. If the domain exists, then registration is returned, including the following fields:
Domain ROID
Domain Name
Domain U-label (if IDN)
Creation Date
Last Updated
Expiration Date
EPP status codes
Registrant Contact Information
Administrative Contact Information
Technical Contact Information
Billing Contact Information (if any)
Sponsoring Registrar ID
Sponsoring Registrar Contact Information
DNS servers (if any)
DNSSEC records (if any)
An example of a domain whois response is included in Appendix 26.1. The Domain ROID is the Repository Object Identifier as described in RFC 5730, §2.8. The ROID field corresponds to the "domain:roid" element of EPP "info" responses.
A domain may be associated with one or more status codes. These are represented in Whois responses as phrases rather than EPP mnemonics. A domain may have any of the following status codes:
PENDING CREATE - a "domain:create" command has been received through the SRS, but the registration has not yet been finalised as an out-of-band review process has not yet been completed.
ADD PERIOD - the domain is in the Add Grace Period
CLIENT HOLD - the registrar has added the clientHold status
DELETE PROHIBITED - this may be present if the domain has either clientDeleteProhibited or serverDeleteProhibited (or both)
INACTIVE - the domain has no DNS servers
PENDING DELETE - the domain has left the Redemption Grace Period and is scheduled for deletion
PENDING DELETE RESTORABLE - the domain is in the Redemption Grace Period
PENDING RESTORE - a restore request has been received, but the Restore Report has not been received
PENDING TRANSFER - there is an active inter-registrar transfer for the domain
RENEW PERIOD - the domain is either in the Renew Grace Period or the Auto-Renew Grace Period
RENEW PROHIBITED - this may be present if the domain has either

clientRenewProhibited or serverRenewProhibited (or both)
SERVER HOLD - the registry has added the serverHold status
TRANSFER PERIOD - the domain is in the Transfer Grace Period
TRANSFER PROHIBITED - this may be present if the domain has either clientTransferProhibited or serverTransferProhibited (or both)
UPDATE PROHIBITED - this may be present if the domain has either clientUpdateProhibited or serverUpdateProhibited (or both)
OK - present if none of the above apply.
The Registrant, Administrative, Technical and Billing Contact sections of the Whois record display the contact information for the contact objects that are associated with the domain. The information displayed replicates the information showed for a contact query (see below). The server shows similar information for the sponsoring registrar.
Domains may have 0-13 DNS servers. If a domain name has no DNS servers, then the "INACTIVE" status code appears in the Status section. If the registrant provided DS records for their DNSSEC-signed domain, then these are included. For each DS record, then the key tag, algorithm, digest type and digest are displayed.

26.3. Contact
Users can query for information about a contact by submitting a query of the form "contact [ID]", where "[ID]" is the contact ID equivalent to the "contact:id" element in EPP "info" responses. This is also the ID used when referring to contacts in domain responses.
The following information is included in Dontact records:
Contact ID
Sponsoring Registrar
Creation Date
Last Updated Date
EPP Status Codes
Contact Name
Organisation
Street Address (1-3 fields)
City
State/Province
Postcode
Country Code (2 character ISO-3166 code)
Phone number (e164a format)
Fax number (e164a format)
Email address
An example of a contact object whois response is included in Appendix 26.2. A contact object may be associated with one or more status codes. These are represented in Whois responses as phrases rather than EPP code mnemonics. A contact object may have any of the following status codes:
DELETE PROHIBITED - present if the contact object has either clientDeleteProhibited or serverDeleteProhibited (or both)
TRANSFER PROHIBITED - present if the contact object has either clientTransferProhibited or serverTransferProhibited (or both)
UPDATE PROHIBITED - present if the contact object has either clientUpdateProhibited or serverUpdateProhibited (or both)
PENDING TRANSFER - there is an active inter-registrar transfer for the contact object
LINKED - the contact object is associated with one or more domain names. A LINKED contact object automatically has the DELETE PROHIBITED status

26.4. Host Objects
Users can query for information about a host object by submitting a query of the form "nameserver [HOST]". The following information is included in host records:
Server Name
IPv4 address (if any)
IPv6 address (if any)
EPP status codes
Sponsoring Registrar

Creation Date
Referral URL (if any)
An example of a host whois response is included in Appendix 26.3. A host object may have an IPv4 or IPv6 address if the host is "in-bailiwick", ie subordinate to a domain name within a TLD operated by the registry. IP address information is not shown for "out-of-bailiwick" hosts.
Host objects may only have two status codes:
INACTIVE - the host is not associated with any domain names
LINKED - the host is associated with one or more domain names
The Referral URL is the website of the Sponsoring Registrar for this host. If the host is subordinate to a domain name in the TLD, this will be the sponsoring registrar of the parent name. If the host is out-of-bailiwick, then the sponsoring registrar is the registrar who issued the original "create" request.

26.5. Character Encoding
Responses are encoded as UTF-8. Queries are assumed to be encoded in UTF-8.

26.6. IDN Support
The Whois service supports Internationalised Domain Names. Users may submit queries for IDN domains using either the U-label or the A-label.

26.7. Bulk Access
CentralNic will provide up-to-date registration data to ICANN on a weekly basis (the day to be designated by ICANN). CentralNic will provide the following data for all registered domain names: 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 it will provide: registrar name, registrar repository object id (roid), hostname of registrar Whois server, and URL of registrar. 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 above.
At ICANN's request, CentralNic will provide ICANN with up-to-date data for the domain names of de-accredited registrar to facilitate a bulk transfer. 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. CentralNic will provide the data within 2 business days.

26.8. Load Projections
As described in §31, CentralNic's existing Whois system receives an average of 0.36 queries per day for each domain name in the registry, including misses for non-existent objects as well as hits.
The number of daily queries per domain for each existing gTLD was calculated using figures for the month of November 2011 published by ICANN. This analysis may be found in Appendix 26.6. It shows little correlation between the number of domains in the TLD and the number of queries that each domain receives. Smaller gTLDs such as .aero and .museum receive more queries per domain than larger gTLDs, but .jobs (which is much larger than either .aero or .museum) received more queries per domain than either. It should be noted that the high volumes observed for .XXX are very likely due to activities surrounding the Landrush and initial launch of that TLD.
CentralNic believes that the query rate observed for its own registry system is mainly affected by its efforts to deter abuse, and outreach to registrars, who often use whois to perform availability checks, to encourage them to EPP instead. CentralNic believes this query rate will also apply for the TLD. A projection of query load for the Whois system for the first 24 months of operation can be found in Appendix 26.4. This model also includes data transit rates and bandwidth projections for the same period. As can be seen, the data and bandwidth requirements are relatively small compared to those for the Shared Registry System and authoritative DNS.

26.9. Technical Implementation
A diagram describing the infrastructure supporting the Whois service may be found in Figure 26.1. During normal operations, the Whois service is operated

at the primary operations centre in London. During failover conditions, it is operated at the Disaster Recovery site in the Isle of Man (see §34).
Queries pass through the firewalls to one of two front-end load balancers. Round-robin DNS distributes queries between the devices. Load balancers are configured in High Availability mode so that if one a server fails, the other will resume service on its IP address until the server can be restored. Queries are distributed to backend application servers via weighted least connections algorithm.

26.9.1. Application Server Architecture
Application servers are built on commodity hardware running CentOS. The service is provided using the mod_whois Apache module (see http://modwhois.sf.net/) which causes Apache to listen on port 43 and accept queries, which are then handled using a PHP script, which generates and returns the response.

26.9.2. Caching
Application servers use caching to reduce database load. Subsequent identical queries are returned a cached record until the cache expires, after which a new record is generated. Records are currently cached for 600 seconds (ten minutes), so if a domain is updated immediately after its Whois record has been cached, the updated record will be visible after ten minutes. This compares favourably to the 60 minute requirement in the gTLD Service Level Agreement. Records are cached in a shared Memached server. Memcached is a high-performance caching server used by some of the largest sites in the world, including Wikipedia, Flickr, Wordpress.com and Craigslist.

26.9.2. Database
The Whois service draws data directly from the primary database. The query volume required to sustain the Whois service is comparable to that of a modest web application such as a small e-commerce site, and as a result a dedicated database for the Whois system is not required. As can be seen in Figure 26.1, a separate logging database is used to aggregate log data for use with the rate limiting system.

26.10. Web based Whois Service
CentralNic provides a web interface to the Whois service on its website. In addition, Applicant will provide a similar service on the TLD registry website. The web Whois acts as a proxy to the port 43 Whois service: users enter a query into a form, and a server-side process submits the query to the Whois server, and displays the response. This service will not be subjected to the rate limiting described above, but users will be required to complete a CAPTCHA to prevent high-volume automated access.

26.11. Searchable Whois Service
Applicant will provide a Searchable Whois Service (SWS). This service will be made available on the TLD website. The SWS provides third parties with a search interface that allows queries for partial matches against a number of domain name properties, including:
domain name (partial match)
registrant name, organisation, address, email
administrative, technical and billing contact information
Nameservers
Nameserver IPv4/IPv6 address
Access to the SWS is restricted. Users must submit an account request via the website, and agree to the terms and conditions which governs their access to the the system. These terms are included as Appendix 26.5. Once their request has been reviewed and approved, they are issued with credentials which permit them to login to the SWS.
To prevent abuse of the SWS, users may only make fifty queries per day initially. This limit can be increased upon request and demonstration of legitimate need.

26.12. Anti-Abuse Mechanisms
CentralNic has implemented measures to mitigate the threat of abuse of the

Whois service. The primary threat to the Whois service are so-called "dictionary" attacks, where an attacker attempts to enumerate the database by flooding the server with queries for domains taken from a precompiled list: as zone files are easy to obtain, this presents a threat to the privacy of contact information in the registry database. The information harvested can be used to compile email databases for spamming, or to send domain renewal scam letters, for example.
The Whois service implements rate-limiting to impede dictionary attacks. For each query, a counter associated with the client IP address is incremented. For subsequent queries, this counter determines the number of queries received within the previous hour. If the number of queries exceeds a pre-set maximum (currently 240 queries per hour), then the server returns an error, warning the user that they have exceeded the permitted query rate. If the user stops sending queries, then eventually the query rate will drop below the limit, and subsequent queries will be permitted. If the user continues to send queries, and the query rate exceeds the limit by a further 25% (300 queries per hour), then the IP address is permanently blocked. For queries over IPv6 (where an attacker might have access to billions of IP addresses), the enclosing /48 will be blocked.
Experience indicates that is an effective mechanism for preventing abuse of the Whois. The rate limit has been tuned to ensure that legitimate uses of the Whois are allowed, but abusive use of the whois is restricted to levels which are unappealing for attackers.
CentralNic keeps a "white list" of IP addresses used by legitimate users of the Whois service, including law enforcement agencies and other research and anti-abuse entities. Registrar access lists are also incorporated into the white list, and IP addresses registered on ICANN's RADAR system will also be included. Queries from IP addresses that appear on the white list are not rate-limited. Interested parties can request addition to the white list by contacting CentralNic's public customer service team.
The web-based Whois does not implement rate-limiting, but users of this service must complete a CAPTCHA to access Whois records.

26.12.1. Denial-of-Service attacks
The rate-limiting system in place provides protection against DoS and DDoS attacks, as any host that attempts to flood the Whois service with queries will be quickly blocked. However, a DDoS attack could still saturate upstream links requiring filtering at the edges of CentralNic's network, as well as their upstream providers. Continuous surveillance and monitoring of the Whois system (see §42) proactively detects these threats. As the Whois service directly queries the primary SRS database, CentralNic rate-limits on the database backend to prevent an attack against the Whois service from disrupting the SRS.

26.13. Monitoring and Logging
Remote monitoring is used to verify the availability of the service and to record the round-trip times for different queries (warm hit, warm miss). Local monitoring records query volumes.

26.14. Resourcing
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to almost one full-time person (83%.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the

TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require 0.22% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.
The Whois service will additionally comply with all requisite data protection laws (with regards to the collection and retention of personal data), including all relevant European Union privacy directives.

27. Registration Life Cycle

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
The lifecycle of a domain in the registry is described in Figure 27.1, and closely follows that of domain names in existing gTLD registries. The lifecycle is described below.

27.1. Available
The domain is not registered. No delegation (or any other records) exist in the DNS, and the whois system will return a "NOT FOUND" response to queries. An EPP "check" command will return an "avail" status of 1.

27.2. Registered
A registar submits an EPP "create" command or registers the domain name via the Registrar Console. The registration fee is deducted from the registrar's balance. The initial registration period may be any whole number of years between one (1) and ten (10).
For five (5) calendar days after the registration of the domain, the registrar can delete the domain and receive a credit for the registration fee (subject to the Add Grace Period Limits Policy).
While the domain is registered, it is delegated to the specified name servers and will resolve normally. During this time, the registrar may update the domain name's DNS settings, lock statuses and contact associations, and may extend the registration period (subject to a maximum of ten (10) years) by submitting a "renew" EPP command or using the Registrar Console.
The domain may also be transferred to a different sponsoring registrar. Upon such transfer the domain name is automatically renewed for one year.

27.3. Expired
When the expiry date is reached, the domain name is automatically renewed for a period of one year, and the renewal fee is deducted from the registrar's account.
For forty-five (45) days after the auto-renewal (Auto-Renew Grace Period), the registrar can delete the domain and receive a credit for the renewal fee.

27.4. Redemption Grace Period
Should the registrar delete the domain, the domain enters the Redemption Grace Period. During this period, the domain name will no longer resolve as all delegation information is removed from the TLD zone.
For the first thirty (30) days after receipt of the delete request, the domain is in the "Pending Delete Restorable" state. During this time, the registrar

may submit an RGP restore request via EPP or the Registrar Console. The domain is then placed into the "Pending Restore" state.
The registrar must then submit an RGP Restore Report detailing the reason why the restore request has been submitted. If the Restore Report is received within five (5) calendar days of the original restore request, then the domain is restored. However, if the Restore Report is not received within this period, then the domain falls back into the "Pending Delete Restorable" state.

27.5. Redemption Period State Diagram
Figure 27.2 describes the state diagram for domain names in the Redemption Grace Period. This diagram is taken from RFC 3915.

27.6. Pending Delete
Forty (40) days after the receipt of the delete request, the domain leaves the "Pending Delete Restorable" and enters the "Pending Delete" status. The registrar cannot submit a Restore Request during this period.

27.7. Released
Five (5) days after the domain enters the "Pending Delete" status the domain name is purged from the database and is once again available for registration.

27.8. Other Grace Periods
The registry also implements the following grace periods. In general, these grace periods allow registrars to delete domain names following billable transactions and receive a refund.

27.8.1. Add Grace Period
As described above, the Add Grace Period (AGP) is the five (5) calendar days following the initial registration of the domain.

27.8.2. Auto-renew Grace Period
As described above, the Auto-renew Grace Period is the forty five (45) calendar days following the auto-renewal of the domain.

27.8.3. Renew Grace Period
The Renew Grace Period is the five (5) calendar days following the renewal of the domain via an EPP "renew" command, or via the Registrar Console.

27.8.4. Transfer Grace Period
The Transfer Grace Period is the five (5) calendar days following the successful completion of an inter-registrar transfer.

27.9. Hold Periods
The registry implements the following hold periods:

27.9.1. Registration Hold Period
The Registration Hold Period forbids inter-registrar transfers of domain names within sixty (60) days of initial registration.

27.9.2. Transfer Hold Period
The Transfer Hold Period forbids transfers of domain names within sixty (60) days of a previous inter-registrar transfer. This Hold Period does not affect disputed transfers that are undone by the registry following the outcome of a Transfer Dispute Resolution process.

27.10. Lock Statuses
The registry system permits the following lock statuses for domain names:

27.10.1. clientHold
This status may be set by registrars using an EPP "update" command, or via the Registrar Console. Domains with this status are removed from the DNS and will not resolve.

27.10.2. clientDeleteProhibited

This status may be set by registrars using an EPP "update" command, or via the Registrar Console. When set, all attempts by the registrar to delete the domain using an EPP "delete" command will be refused with EPP response code 2304 (Status Prohibits Operation). Registrars must remove the code using an EPP "update" command before they can delete the domain.

27.10.3. clientRenewProhibited
This status may be set by registrars using an EPP "update" command, or via the Registrar Console. When set, all attempts by the registrar to renew the domain using an EPP "renew" command will be refused with EPP response code 2304 (Status Prohibits Operation). Registrars must remove the code using an EPP "update" command before they can renew the domain.

27.10.4. clientUpdateProhibited
This status may be set by registrars using an EPP "update" command, or via the Registrar Console. When set, all attempts by the registrar to update the domain using an EPP "update" command will be refused with EPP response code 2304 (Status Prohibits Operation), unless the "update" request frame includes a "rem" element to remove this status. Once the status has been removed, subsequent "update" commands will succeed.

27.10.5. clientTransferProhibited
This status may be set by registrars using an EPP "update" command, or via the Registrar Console. When set, all attempts by other registrars to submit a transfer request for the the domain using an EPP "transfer" command, or via the Registrar Console, will be refused with EPP response code 2304 (Status Prohibits Operation). The sponsoring registrar must remove this status before any other registrar can submit a transfer request.

27.10.6. serverHold
This status is set by the registry in accordance with policy. It cannot be removed by registrars. Domains with this status are removed from the DNS and will not resolve.

27.10.7. serverDeleteProhibited
This status is set by the registry in accordance with policy. It cannot be removed by registrars. When set, all attempts by the registrar to delete the domain using an EPP "delete" command will be refused with EPP response code 2304 (Status Prohibits Operation).

27.10.8. serverUpdateProhibited
This status is set by the registry in accordance with policy. It cannot be removed by registrars. When set, all attempts by the registrar to update the domain using an EPP "update" command will be refused with EPP response code 2304 (Status Prohibits Operation).

27.10.9. serverRenewProhibited
This status is set by the registry in accordance with policy. It cannot be removed by registrars. When set, all attempts by the registrar to renew the domain using an EPP "renew" command will be refused with EPP response code 2304 (Status Prohibits Operation).

27.10.10. serverTransferProhibited
This status is set by the registry in accordance with policy. It cannot be removed by registrars. When set, all attempts by the registrar to transfer the domain using an EPP "transfer" command will be refused with EPP response code 2304 (Status Prohibits Operation).

27.11. Lifecycle Processing
Domain names move through the lifecycle in one of two ways: in real-time as a result of registrar activity, or during daily billing runs.
Billing runs take place once per day. The billing run performs the following batch jobs:
auto-renewal of expired domains

processing of registration and renewal fees for domains that move outside their grace periods
processing of domains in the RGP state (from restorable to not restorable, checking for missing restore reports, etc)
purging of domains scheduled for deletion
The billing runs also perform registrar account management functions such as generation of invoices, sending balance warnings, and generation of internal reports.

27.12. Inter-Registrar Transfer Period
When a transfer request is received, the action date of the transfer is set to five (5) calendar days from the moment of the original request. Successful transfers are approved at the end of this period.

27.13. pendingCreate Status
The Registry system supports the "pendingCreate" status for domain names, as described in RFC 5731, §3.3. Domains in this state are fully registered in the database (subsequent "create" commands would fail with an Object Exists error) but are not present in the DNS.
This status is used when a particular TLD implements a policy whereby registration requests are verified by a third party such as a Sponsoring Organisation or Validation Agent. Following out-of-band review of the request, the registration may be approved or denied.
If a request is denied, then the domain is immediately purged from the registry system, and the registrar notified via email and the EPP message queue. The registrar also receives a credit for the registration fee. If approved, then the pendingCreate status is removed from the domain which begins to resolve.

27.14. Resourcing
The domain registration lifecycle is managed through automated backend processes that generally require no human intervention, and real-time business logic implemented in Shared Registry System application code. Operations personnel will be responsible for maintaining and developing the computing infrastructure which supports the lifecycle processing systems. Backend systems are hosted on a flexible virtual infrastructure hosted at the primary operations centre at the Goswell Road Data Centre in London.
The domain registration lifecycle does have customer and registrar support requirements, so a proportion of the time of the Operations Manager, Support Manager and Support Agent has been dedicated to this area. This time primarily relates to dealing with questions and comments from registrars and registrants about the status of their domain names.
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to 30% of a full time person. Because of the maturity and stability of this system (which has been in use for more than 16 years), only 5% of time of a technical developer has been allocated to this area.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support

up to 4.5 million domain names. Therefore the TLD will require 0.22% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

28. Abuse Prevention and Mitigation

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
Top Level Domain registries stand in a unique position within the global DNS infrastructure.
TLD registries collect registrants' registration data and so often "know" the entity responsible for a particular domain name. TLD registries record associations between domain names, registrars and registrants and therefore are in the core of the control chain for every domain name in the TLD. Registries also directly control the delegation records and therefore have the power to enable or disable a particular domain name in the DNS.
This unique position gives power and calls for responsibility. Applicant as a future TLD registry recognizes its important role in maintaining law and order and is committed to acting in the best interests of the public.
Hereby we provide a description of the principles and procedures we will apply to mitigate abusive conduct.

28.1. Single Abuse Point of Contact
To streamline the information flow and to facilitate ease of communication with the public, Applicant will dedicate a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the TLD. The contact information will consist of at least an email address and a telephone number. This point of contact will be prominently published on the registry website by the commencement of the Sunrise period.
Applicant will ensure that:
The e-mail account is continuously monitored and all communication securely stored
The telephone number is either answered by a live person or diverted to a monitored voicemail account.
Abuse contact information will be kept current and will be updated should it ever change in a timely manner
Messages received through the published abuse point of contact will be processed via the same procedure and within the same timeframe as the signals coming from the monitoring systems. Each message, both via email and phone channels, triggers the creation of a support ticket in a dedicated queue and procedures for ticket escalation exist. Messages originating from law enforcement authorities are by default assigned an escalated level. For critical tickets personnel is available 24x7 to react accordingly.
Applicant and CentralNic commit to responding to all abuse complaints within 24 hours of receipt (on a 24x7 basis). During the time periods when its global offices are open (typically 8am-6pm in London, Los Angeles and Dubai) response times are expected to be substantially faster, at around 2-3 hours.

28.2. Policy on Handling Complaints Regarding Abuse
Applicant is prepared to deal with situations where registry intervention may be required in order to stop illegal activity, prevent abusive conduct or to enforce the law.
Applicant will adopt a comprehensive Acceptable Use Policy that will establish what constitutes acceptable use of the domain and will contain a description of

procedures registry that will apply to enforce the Policy. The initial policy is provided in answer to question 29.
An enforcement action may be triggered by a variety of events including complaints from the public, registrars or ICANN, decisions of a competent dispute resolution provider, outreach from a governmental agency or findings produced by internal investigation or monitoring processes.
Normally if abusive behaviour in a TLD is encountered, the reports of such behaviour and the evidence available will be analysed by the Registry. If the Registry, in its sole discretion, concludes that a Domain Name Holder has indeed violated a TLD Policy, the registrant will be given a notice and opportunity to correct the breach.
Furthermore, the registry reserves the right to lock the domain name or put it on hold (preventing domain resolution in the DNS). In extreme cases where a domain is involved in malicious or illegal activity there are provisions for rapid takedown of the domain name in question. The situations in which rapid takedown provisions may be applied, include, but are not limited to:
Phishing
Pharming
Distribution of illegal content
Distribution of malware
Fast flux hosting
Botnetting
Unauthorized access to information systems
Threats to the security and⁄or stability of the TLD
The Acceptable Use Policy will be incorporated into the Registry-Registrar agreements and Registrars will be required to pass through the requirements to comply with the policy to the registrants.
Applicant will take reasonable steps to investigate and respond to any reports of illegal activity in connection with the use of the TLD and will cooperate with the competent governmental agencies in such investigations.
Applicant will utilize the expert services of its registry services provider CentralNic to implement and enforce all of our anti-abuse policies in our TLD. CentralNic has dedicated and scalable resources for this function, described below.
CentralNic has long experience in the domain registry business, and is an industry leader with respect to its anti-abuse policies. CentralNic has a dedicated Dispute Resolution Policy in place with WIPO, found at WIPO's website: http:⁄⁄www.wipo.int⁄amc⁄en⁄domains⁄gtld⁄cnic⁄index.html.
This policy mirrors the UDRP policy for new gTLDs and, as a result, CentralNic already has real-time experience working with WIPO to implement and execute a similar policy.
CentralNic has trained personnel who handle interaction with WIPO, to ensure that panelists' decisions are carried out expeditiously as required by the DRP.
CentralNic also enforces a Policy on Phishing and Fraud, found at its dedicated Phishing & Abuse page at the following website: https:⁄⁄www.centralnic.com⁄support⁄abuse. Pursuant to clause 13, sections (f) and (h) of CentralNic's Terms and Conditions, CentralNic may cancel the registration or suspend registration of a domain name:
(f) if CentralNic believes that the domain name was registered for use in a "phishing" attack or other illegal activity of any kind.
(h) if inaccurate or false contact details are provided.
Further to these conditions, CentralNic operates the following policy regarding suspected "phishing" domain names:
- If we have a reasonable suspicion that a domain name registered at CentralNic is being used in a phishing attack, or otherwise being used for other illegal activities, we will place the domain name "On Hold" and under a Registry Lock.
- We will then notify the current registrar for the domain name. If the registrar can provide confirmation that the domain name was registered in "good faith" by the registrant, then CentralNic will immediately unlock the domain name and place it on the "Live" status. - If no confirmation is received, or the registrars agree that the domain name was registered in "bad faith", the domain name will be placed onto "Pending Deletion", and will be fully deleted from the database after 45 days.

28.3. Orphan Glue
CentralNic's registry system includes effective measures to prevent the abuse of orphan glue records.
Firstly, the Shared Registry System will reject any request to create host object that is the child of a non-existent domain name. That is, if EXAMPLE.TLD does not exist, then NS0.EXAMPLE.TLD cannot be created. If the parent domain name does exist, then only the sponsoring registrar of that domain is permitted to create child host objects.
CentralNic's registry system currently follows the third model described in the SAC 048 report: orphan glue records are deleted from the registry and removed from the DNS when the parent domain name is deleted. If other domains in the database are delegated to orphan hosts that are removed, then the delegation is also removed from these domains.

28.4. Measures to Maintain Whois Accuracy
Applicant will operate a "thick" WHOIS system, in which all registrants' contact information will be stored in a single database maintained by the registry. Accredited registrars will have the ability to change the records in that database through the Shared Registration System. The Registry-Registrar agreement requires registrars to ensure that the WHOIS data is accurate at the time of submission and also requires the information provided on the system to be updated in a timely manner in case of any changes. Corresponding provisions also exist in the Registrar Accreditation Agreement (RAA), para. 3.7.7.
In addition to the standard measures described above, the .TLD WHOIS system will feature extra levels of reliability with regards to Whois information.

28.4.1. Extra checks on WHOIS data
Applicant, through its Registry-Registrar agreements will require registrars to perform the following additional checks on the WHOIS data:
Verify syntactic correctness of email addresses and phone numbers by validating them against the corresponding standards
Verify that the domain holder receives email at the addresses listed in WHOIS as registrant's email address and administrative contact email address, by requiring them to click a unique web link that is sent to those addresses.
28.4.2. Random audits of WHOIS records by the Registry
Applicant will periodically (at least once every 12 months) perform a random check of WHOIS records in .TLD for prima facie evidence of fraudulent or inaccurate WHOIS information. For those suspicious records that may be found, Applicant will further require registrars to conduct a reasonable investigation and to respond with one of the three possible actions:
confirm that the information provided in WHOIS is accurate, or
correct the WHOIS information, or
delete the domain name(s).
The measures described above exceed the ICANN requirements and are adequate to improve accuracy of WHOIS information while maintaining low implementation cost for registrars and good user experience for registrants.

28.5. Resourcing
Applicant and CentralNic will provide abuse response on a 24x7 basis. The resourcing to fulfill this function will be provided by a combined team of support and operations personnel. The first response function will be provided by support agents during normal office hours, with this responsibility being passed to the Network Operations Centre(NOC) during 24x7 operations.
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to 75% of a full-time role.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure,

then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require 0.22% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

28.6. Periodic review of anti-abuse policies
Applicant acknowledges that new types of abusive behaviour emerge in cyber space and is prepared to take steps to counter any new types of abuse. Applicant will periodically (once every 12 months, or more frequently depending on the circumstances) require CentralNic to provide reports regarding the received abuse-related complaints. Such reports should contain categorisation of the abusive behaviour reported, actions taken and response time. Applicant will analyse the reports and will review its anti-abuse policies to continually improve the handling of abuse complaints.

29. Rights Protection Mechanisms

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
This policy is subject to all ICANN requirements for new gTLDs, including the URS and UDRP, and will be made compliant with any future ICANN requirements as and when necessary.
Applicant recognizes providing appropriate mechanisms to protect legal rights of others as one of the core objectives of the Registry. Applicant will follow rules and policies developed by ICANN with regards to Rights Protection Mechanisms (RPMs). Applicant will fully comply with Specification 7 of the new gTLD registry agreement and will provide additional rights protection mechanisms over and above the ICANN requirements. Both standard and additional RPMs are described below.

29.1. Sunrise Period
Prior to the open registration phase Applicant will offer a priority registration period for owners of trademarks and service marks. This period will last at least 30 days.
Applicant will support Trademark Clearinghouse (TCH) once it is implemented by ICANN. Owners of trademarks pre-validated by the Clearinghouse will be able to secure their domain registrations during the Sunrise period without further verification of their intellectual property rights.
The flowchart of the Sunrise and eligibility validation process is available in Figure 24.4.

29.1.1. Sunrise Eligibility Requirements
Any entity that holds a trademark or service mark will be qualified to register a domain during the Sunrise period. Registrations obtained during the Sunrise Period will be subject to challenge as described below.
As a minimum, the Registry will recognize as qualifying all word marks that:

Are nationally or regionally registered and for which proof of use is available, or
Marks that have been validated by the court, or
Marks that are specifically protected by a statute or treaty.
All the Sunrise Eligibility requirements will have to be met by the cut-off date which will be announced in due course.
Full details of the Sunrise registration process will be finalized after the Trademark Clearinghouse service is implemented and full documentation, policies, terms and conditions are made available. For guidance, data items that will need to be provided by the qualifying applicant to apply for a .Feedback Sunrise registration are listed below:
name or description of the trademark
registration number
registration date
country of registration
capacity of the applicant
reference to the Trademark Clearinghouse database record
Representation that the information provided is true and correct

29.1.2. Sunrise Challenge Process
The result of the evaluation of Sunrise applications will be published on the Registry website. A process will be in place to allow third parties to dispute the registrant rights to own a domain name. Applicant will engage with a reputable adjudicator to manage the Sunrise challenge process. The adjudicator will charge a reasonable fee for Sunrise challenges.
The Sunrise Challenge rules will allow challenges based on at least the following four grounds:
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;
the domain name is not identical to the mark on which the registrant based its Sunrise registration;
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
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.

29.2. Trademark Claims Service
The Trademark Claims service will be launched by the registry as soon as the open registration period starts and will be provided for at least 90 days (exceeding the period mandated by ICANN). The Applicant will review the effect of the Trademark Claims service and based on the results of such review Applicant is prepared to consider providing the Trademark Claims service on an ongoing basis.
The essence of the Trademark Claims service is as follows: if a domain name registration is attempted for which there exists a matching record in the Trademark Clearinghouse database, then the prospective registrant will be presented with a notice that third party trademark rights exist for a matching designation and will be required to provide a statement that to the best of his or her knowledge, the registration and use of the requested domain name will not infringe on the rights of the trademark holders.
If the registrant chooses to proceed with the registration, the corresponding trademark holder(s) will be notified that such registration has taken place.
Operational rules of the Trademark Claims service are heavily dependent on the specific implementation of the Trademark Clearinghouse which is not yet available in writing. Therefore full details of the Trademark Claims service will be finalized after the TCH is implemented by ICANN and full documentation, policies, terms and conditions become available.

29.3. Uniform Domain Name Dispute Resolution Policy (UDRP)
The Uniform Domain Name Dispute Resolution Policy is an ICANN consensus policy

for adjudication of disputes between domain name holders and owners of matching trademarks. Every registrant must agree to this mandatory administrative procedure in its Domain Registration Agreement with the registrar. Registrars have certain responsibilities to facilitate adjudication of UDRP disputes and to enforce the decisions of the arbitration panels.
.Feedback will comply with the Uniform Domain Name Dispute Resolution Policy or with any successor thereof. The UDRP will be incorporated by reference into Registry-Registrar Agreements. Similarly, Registrars will be required to incorporate it into their Domain Registration agreements with the Registrants. The UDRP process does not provide for any participation by the Registry and is fully borne by the Registrar, Registrant, Complainant and the Dispute Resolution Provider. However, Applicant is prepared to collaborate with all relevant stakeholders to ensure UDRP decisions are implemented.
CentralNic, Applicant's registry services provider, has maintained a similar dispute resolution policy with WIPO which is available at http://www.wipo.int/amc/en/domains/gtld/cnic/index.html. CentralNic has dedicated personnel trained to address these types of complaints and to communicate with WIPO and other relevant stakeholders.

29.4. Uniform Rapid Suspension System (URS)
The Uniform Rapid Suspension System (URS) described in the ICANN gTLD Applicant Guidebook is a new Rights Protection Mechanism for rapid takedown of domain names that by clear and convincing evidence infringe on legitimate trademark rights of third parties.
As opposed to the UDRP procedure, registries are required to participate in the URS procedure and enforcement of the URS decisions. Applicant will comply with the URS policy once implemented by ICANN.
The current URS procedure as described in the Applicant Guidebook is as follows: within 24 hours of receipt of the Notice of Complaint from a URS Provider, the Registry has to lock the domain, restricting all changes to the registration data, including transfer and deletion. The domain name will continue to resolve at this stage. The Registry will notify the URS Provider immediately upon locking the domain name.
If the URS Determination is in favour of Complainant, upon receipt of the Determination the Registry will suspend the domain name which is intended to remain suspended for the balance of the registration period and will not resolve to the original web site. Instead, the nameservers will be redirected to an informational web page provided by the URS Provider about the URS. The Whois record for the domain name will continue to display all of the information of the original Registrant except for the redirection of the nameservers. In addition, the Whois will reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration.
If the URS Determination is in favour of the Respondent, the Registry will remove the lock status from the domain name allowing the registrant to continue using it normally.
The URS compliance function will be performed by CentralNic and overseen by the Applicant. Given CentralNic long-standing experience in dealing with trademark-related disputes in domain names, Aplicant has no doubt that this function will be performed by CentralNic flawlessly.

29.5 Mediation
CentralNic has implemented a solution that complements the UDRP by adopting a best practice of Nominet and other ccTLDs. CentralNic has experienced a high percentage of domain disputes resolved without the need for filing a formal and relatively expensive UDRP complaint, by offering informal mediation to any person or entity who submits a Request for Mediation to the registry. The Mediation rules that CentralNic intends to apply to gTLDs are copied below:
"CentralNic" means CentralNic Ltd, 35-39 Moorgate, London EC2R 6AR, United Kingdom.
"Complainant" means the party submitting a Request for Mediation concerning a Domain Name registration pursuant to the CentralNic Mediation Rules.
"Domain Name" means any domain name registered under a sub-domain provided by CentralNic.

"Mediation" means a mediation conducted by CentralNic in accordance with the CentralNic Mediation Rules that are incorporated by reference and made a part of the Registration Agreement.
"Party" means a Complainant or a Respondent.
"Registration Agreement" means the agreement between CentralNic and a Domain Name holder.
"Respondent" means the holder of a Domain Name registration in respect of which a Request for Mediation is submitted pursuant to the CentralNic Mediation Rules.
1. Request for Mediation: (a) Any person or entity may submit a Request for Mediation relating to a Domain Name registration in accordance with the CentralNic Mediation Rules. A copy of the Request for Mediation shall be sent to the Respondent and to CentralNic. (b) The Request for Mediation shall be submitted in writing by e-mail and shall: (i) State that the Complainant wishes to submit the dispute to Mediation in accordance with the CentralNic Mediation Rules; (ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the Mediation; (iii) Specify a preferred method for communications directed to the Complainant in the Mediation (including person to be contacted, medium, and address information); (iv) Provide the name of the Respondent and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact the Respondent or any representative of the Respondent, including contact information based on pre-Request dealings; (v) Specify the Domain Name(s) that is⁄are the subject of the Request; (vi) Contain a brief statement of the nature of the dispute. (c) The Request for Mediation may relate to more than one Domain Name, provided that the Domain Names are registered by the same Domain-Name holder.
2. Commencement: (a) The date of commencement of the Mediation shall be the date on which the Request for Mediation is received by CentralNic. (b) CentralNic shall inform the Parties of the receipt by it of the Request and of the date of commencement of the Mediation.
3. Mediation: (a) CentralNic shall conduct the Mediation in a manner which CentralNic, in its sole discretion, considers appropriate. (b) The language of the Mediation shall be English, unless decided otherwise by CentralNic. (c) CentralNic will not reveal details of the Mediation to any third parties unless ordered by a court of competent jurisdiction or required by applicable laws or regulations or except as may be provided under the CentralNic Dispute Resolution Policy and the Rules for CentralNic Dispute Resolution Policy.
4. Termination of the Mediation: The Mediation will terminate ten (10) calendar days after the date of commencement. At the request of the Parties or on its own motion, CentralNic may, in exceptional cases, extend the period of time for the Mediation. The fact of termination shall be recorded by CentralNic.
5. Fees: No fees shall be payable by either party for the conduct of the Mediation.
6. Exclusion of Liability: Except in the case of deliberate wrongdoing, CentralNic shall not be liable to a Party for any act or omission in connection with the Mediation.
7. Waiver of Defamation: The Parties agree that any statements or comments, whether written or oral, made or used by them or their representatives in preparation for or in the course of the Mediation shall not be relied upon to found or maintain any action for defamation, libel, slander or any related complaint, and this Paragraph may be pleaded as a bar to any such action.
8. Amendments: CentralNic reserves the right to modify these Rules at any time. CentralNic will post the revised Rules at at least thirty (30) calendar days before they become effective. The version of these Rules in effect at the time of the submission of the Request for Mediation to CentralNic shall apply to the Mediation commenced thereby.
Applicant notes this is CentralNic's current policy for its current registry businesses. Applicant may make modifications to this Policy, without limitation by charging a reasonable fee and⁄or by specifying the mediation mechanism, as its business plans develop prior to launch of the TLD. However, Applicant remains committed to offering a less formal and less expensive procedure than the UDRP, and perhaps even the URS, to the extent commercially feasible.

29.6 Abusive use/takedown policies
Answer to question 28 contains a detailed description of measures that the Applicant will take to prevent and mitigate abusive registrations and the description of policies that the Applicant will apply to handle complaints regarding abuse and take down abusive registrations. To summarise,
Applicant will dedicate a single abuse point of contact. Correspondence and complaints coming through that point of contact will be continuously monitored and responded to within 24 hours
Applicant will adopt a comprehensive Eligibility and/or Acceptable Use Policy that will set forth the limits of acceptable use of domains and the procedures the Registry will apply in case of violations of applicable laws or policies, including takedown procedures. The initial Acceptable Use Policy is provided in this section below.
Applicant will delete orphan glue records once the parent domain is deleted to prevent abuse of these orphan glue records
Applicant will require registrars to perform extra checks on WHOIS data to improve its accuracy
Applicant will perform random audits of WHOIS data and will flag suspicious registrations via registrars

29.7. Post-Delegation Dispute Resolution Procedure
Applicant reaffirms its intent to comply with the ICANN-mandated Post-Delegation Dispute Resolution Procedure (PDDRP).
Applicant believes that its choice of TLD string and the way the TLD is intended to be operated represents a good faith offering of Top Level Domain Registry service and does not infringe on any legitimate third party trademark rights.

Applicant also reaffirms its commitment to maintain .Feedback free of violations of third party trademark rights through second level domain registration and use. Applicant has all the required resources, policies and procedures in place to address any situations of abuse without the need to invoke the PDDRP procedure.

29.8. Resourcing
The Rights Protection Mechanisms described above include a combination of both technical and non-technical systems: for example, the Trademark Claims Service may (depending on the final specification published by ICANN) require development, maintenance and support of an EPP extension, as well as real-time integration with the TCH API, whereas the UDRP is a primarily manual process of managing and responding to communications from complaints, respondents and UDRP service providers.
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to half of a full-time role.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. After three years of operation, the optimistic projection for the TLD states that there will be 10,000 domains in the zone. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require 0.22% of the

total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

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

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.
30(a).1. Introduction
CentralNic's Information Security Management System (ISMS) complies with ISO 27001. CentralNic is working towards achieving full ISO 27001 certification and has secured the services of Lloyd's Register Quality Assurance (LRQA), a UKAS accredited certifier for its ISO 27001 certification. A letter from LRQA confirming this engagement is included in Appendix 30(a).1. Stage One of this process is scheduled during May 2012, with Stage Two occurring in July 2012. The ISMS is part of a larger Management System which includes policies and procedures compliant to ISO 9001.

30(a).2. Independent Assessment
As part of ISO 27001 compliance, CentralNic's security policies will be subjected to annual external audit. Further details can be found in §30(b).

30(a).3. Augmented Security Levels
Applicant believes that the TLD requires no additional security levels above those expected of any gTLD registry operator. Nevertheless, Applicant and CentralNic will operate the TLD to a high level of security and stability in keeping with its status as a component of critical Internet infrastructure. Registry systems are hardened against attack from external and internal threats. Access controls are in place and all systems are monitored and audited to mitigate the risk of unauthorised access, distribution or modification of sensitive data assets. The Authoritative DNS System has been designed to meet the threat of Distributed Denial-of-Service (DDoS) attacks by means of over-provisioning of network bandwidth, and deployment of Shared Unicast ("Anycast") addresses on nameservers. Whois services have been designed with built-in rate limiting and include mechanisms for protection of personal information. The stability of the registry is supported by use of high-availability technologies including a "hot" Disaster Recovery site in the Isle of Man, as well as a backup provider relationship with GMO Registry in Japan.

30(a).4. Commitments to Registrars
Applicant and CentralNic will make the following commitments to the TLD registrars:
The SRS will be operated in a secure manner. Controls will be in place to prevent unauthorised access and modification of registry data.
The Whois service will prevent unauthorised bulk access to domain name registration data, and provide tools to protect personal information.
The DNS system will be designed to provide effective defence against DDoS attacks. The registry will proactively monitor the DNS system to provide early warning against threats to the stability of the TLD.
The DNSSEC system will be operated in accordance with best practices and recommendations as described in the relevant RFC documents (described in §43).
Security incidents reported by registrars, registrants and other stakeholders will be acted upon in accordance with the Security Incident Response Policy (see below).
Security vulnerabilities reported to the registry will be acknowledged and

remediated as quickly as possible.
Registrars will be promptly notified of all incidents that affect the security and stability of the registry system and their customers, and will be kept informed as incidents develop.

30(a).5. Access Controls
CentralNic operates an access control policy for the registry system. For example, the web-based Staff Console which is used to administer the SRS and manage registrar accounts supports a total of ten different access levels, ranging from "Trainee", who have read-only access to a subset of features, to "System Administrator" who have full access to all systems.
Underlying server and network infrastructure is also subjected to access control. A centralised configuration manager is used to centrally control access to servers. Individual user accounts are created, managed and deleted via the configuration server. Access to servers is authenticated by means of SSH keys: only authorised keys may be used to access servers. Operations personnel can escalate privileges to perform administration tasks (such as updating software or restarting daemons) using the "sudo" command which is logged and audited as described below.
Only operations personnel have access to production environments. Development personnel are restricted to development, staging and OT&E environments.

30(a).6. Security Enforcement
Security controls are continually monitored to ensure that they are enforced. Monitoring includes use of intrusion detection systems on firewalls and application servers. Attempted breaches of access controls (for example, port scans or web application vulnerability scans) trigger NOC alerts and may result in the execution of the Security Incident Response Policy (see below).
Since CentralNic operates a centralised logging and monitoring system (see &sect42;), access logs are analysed in order to generate access reports which are then reviewed by NOC personnel. This includes access to servers via SSH, to web-based administration systems, and to security and networking equipment. Unexpected access to systems is investigated with a view to correcting any breaches and⁄or revoking access where appropriate.

30(a).8. Security Incident Response Policy
CentralNic operates a Security Incident Response Policy which applies to all events and incidents as defined by the policy, and to all computer systems and networks operated by CentralNic.
The Policy provides a mechanism by which security events and incidents are defined (as observable change to the normal behaviour of a system attributable to a human root cause). It also defines the conditions under which an incident may be defined as escalated (when events affect critical production systems or requires that implementation of a resolution that must follow a change control process) and emergencies (when events impact the health or safety of human beings, breach primary controls of critical systems, or prevent activities which protect or may affect the health or safety of individuals).
The Policy established an Incident Response Team which regularly reviews status reports and authorises specific remedies. The IST conduct an investigation which seeks to determine the human perpetrator who is the root cause for the incident. Very few incidents will warrant or require an investigation. However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.
The Policy makes use of CentralNic's existing support ticketing and bug tracking systems to provide a unique ID for the event, and means by which the incident may be escalated, information may be reported, change control processes put into effect, and ultimately resolved. The Policy also describes the process by which an incident is escalated to invoke an Emergency Response, which involves Lock-Down and Repair processes, monitoring and capturing of data for forensic analysis, and liaison with emergency services and law enforcement as necessary.

30(a).9. Role of the Network Operations Centre (NOC)

In addition to its role in managing and operating CentralNic's infrastructure, the NOC plays a key role in managing security. The NOC responds to any and all security incidents, such as vulnerability reports received from registrars, clients and other stakeholders; monitoring operator and security mailing lists (such as the DNS-OARC lists) to obtain intelligence about new security threats; responding to security-related software updates; and acting upon security alerts raised by firewall and intrusion detection systems.

30(a).10. Information Security Team
CentralNic maintains an Information Security Team (IST) to proactively manage information security. The IST is a cross-functional team from relevant areas of CentralNic. These key members of staff are responsible for cascading rules, regulations and information to their respective departments. They are also the first port of call for their departmental staff to report potential security incidences and breaches, the IST are all members of an internal email group used to co-ordinate and discuss security related issues.
The IST is comprised of the CEO, CTO, Operations Manager, Senior Operations Engineer and Security Engineer.
IST responsibilities include:
Review and monitor information security threats and incidents.
Approve initiatives and methodologies to enhance information security.
Agree and review the security policy, objectives and responsibilities.
Review client requirements concerning information security.
Promote the visibility of business support for information security company-wide.
Manage changes to 3rd party services that may impact on Information Security
Perform internal audits with the assistance of Blackmores.

30(a).11 Auditing and Review
ISO 27001 includes processes for the auditing and review of security systems and policies. Audits are performed annually by an independent assessor. The IST periodically reviews the ISMS and conducts a gap analysis, identifying areas where performance does not comply with policy, and where the Risk Assessment has identified the need for further work.

30(a).12. Testing of Controls and Procedures
CentralNic will conduct bi-annual penetration tests of its registry systems to ensure that access controls are properly enforced and that no new vulnerabilities have been introduced to the system. Penetration tests will include both "black box" testing of public registry services such as Whois and the Registrar Console, "grey box" testing of authenticated services such as EPP, and tests of physical security at CentralNic's offices and facilities. CentralNic will retain the services of a reputable security testing company such as SecureData (who, as MIS-CDS, performed the 2009 assessment of CentralNic's security stance). The results of this test will be used in annual reviews and audits of the ISMS.

30(a).13. Applicant Security Policy
Fegistry has physical security measures including locked offices, visitor log, etc). Fegistry uses best practices in computer security (screen locks, password policy, & antivirus updates done regularly). Fegistry has network security (firewalls, secured wifi, secured cabling and network cabinets, network activity logging). Fegistry uses data security (encrypted storage of files and credentials).
Fegistry is working with CentralNic and other security experts to enhance site and network security measures in addition to policy development, employee training, and enhanced physical security measures.

crowell moring

Annex 6.

New gTLD Application Submitted to ICANN by: DotHotel Inc.

String: hotel

Originally Posted: 13 June 2012

Application ID: 1-1059-97519

Applicant Information

1. Full legal name

DotHotel Inc.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

http://www.radixregistry.com

Primary Contact

6(a). Name

Mr. Brijesh Harish Joshi

6(b). Title

Director & GM

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

Mr. Namit Sunil Merchant

7(b). Title

General Manager

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

International Business Company

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

International Business Companies Act, 1994

Republic of Seychelles

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.

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

Brijesh Joshi	Director & GM

Vishal Manjalani	Director & VP

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

Bhavin Turakhia	Founder
Brijesh Joshi	Director & GM
Namit Merchant	General Manager
Vishal Manjalani	Director & VP

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

Radix FZC	Not Applicable

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

Applied-for gTLD string

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

hotel

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.

We have engaged ARI Registry Services (ARI) to deliver backend technology services for this TLD.

ARI is experienced with:
- The operational issues of operating TLDs, including ccTLDs.
- TLDs that offer registrations at the third level (e.g. .com.au, .net.au) and which have their own set of unique issues.
- The rendering and operational issues surrounding the introduction of IDNs.
The following is the result of ARI's analysis.

1. INTRODUCTION

ARI has not found any issues unique to this TLD with respect to operational and rendering issues.

This has been established by:
- Testing of the TLD string itself.
- Researching issues experienced by others.
- Our understanding of published material.
- Our own experience.

2. LOCAL TESTING OF THE TLD STRING

ARI has executed a suite of tests to evaluate any issues arising from the use of the TLD string. ARI configured a test environment that consisted of DNS software that served authoritative responses for this TLD, web server software that hosted a simple website, and an email server that provided mailboxes for sample domains in this TLD. Testing included:
- Navigation of websites using the address bar and hyperlinks.
- Composition and delivery of mail.
- Mail filters such as spam detection.
- Display of domain names in address bars, hyperlinks, and free text.
Where possible, ARI attempted to test many equivalent applications, however the number of and different versions of applications means that testing was limited to the more common environments. Tested platforms and applications included:
- Microsoft Windows, Apple OS X and Red Hat Linux.

- Internet Explorer, Safari, Opera, Firefox and Chrome.
- Exchange, Sendmail and Postfix.
ARI did not find any operational or rendering issues with this TLD that are unique to this TLD.

This completes our response to Q16.

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.

MISSION AND PURPOSE:

The mission of .Hotel is to represent the global hotel industry on the Internet. We envision Hotel owners of all sizes, and from all over the world, using .Hotel as a medium to easily reach out to customers.

Although there are several indicators, it is difficult to accurately size our market. Global travel portals such as "Expedia.com" (^1) and "Hrs.com" (^2) claim to offer booking options for 140,000+ and 250,000+ hotels worldwide respectively. .Travel in their application (^3) to ICANN has claimed that about 550,000 + Hotels and resorts exist worldwide.

These figures give us ballpark estimates of the number of Hotels worldwide that could fall under our addressable market. It is difficult to use this range to size our market since each source gives us a different estimate, and the variances are high. There is also a high degree of 'double counting' where multi-chain hotels are being counted once for each hotel they operate, while all properties within their chain only use one website and domain name.

We arrived at our addressable market for .Hotel, based on a thorough analysis of the existing Domain names in for Com, Net, Info, Biz and Org, that have the term 'hotel' as a part of the domain name. This is a public source that directly correlates the actual domain names related to the word 'Hotel' existing out there amongst top gTLDs, and we believe this to be the most reliable and relevant methodology.
This result was 525,913 domain names which have the term 'hotel' as a part of the domain name. This most accurately represents the size of our target market.

The Global Hotel Industry is exhibiting an improving economic scenario, although it is evident that the global recession did have an impact. As per the latest Smith Travel & Research (STR) Report - August, 2011, over the last two years, there has been a cumulative growth of 3% in revenue, 5% in demand, and another 5% in occupancy rates. In a recent interview to the Wall Street Journal(^4), Arne Sorenson, President and CEO of the Marriot International, stated "…when you look at what's actually happening in the hotels, people are travelling, businesses are travelling, businesses are investing and business conditions are actually looking good."

Current trends also suggest that developing markets are enjoying a higher share of this positivity. As per the recent "Global Hotel Industry Outlook Survey 2011-12" (Ref. Code: ICDR1223, World Market Intelligence Panel report, published June 2011), China, India and Brazil are expected to be the emerging markets which will register the most growth. Take the Indian market for instance - The Indian Hotel industry experienced a healthy CAGR (Compounded annual growth rate) of 11 percent during 2005-2009, raking in revenues of over $3.8 Billion in 2009 (IBEF Report Nov 2011) (^5). Globally, over the next two years occupancy growth is expected to be above the average for the last 5 years.

All of these factors indicate the need for Hoteliers to stay on their toes, find new means of innovation, differentiation and branding. A Namespace that represents them will provide a strong weapon in their arsenal to ensure they continue to thrive. After all, a Hotel is more than a temporary home for travelers. It's only fair that they get their own home on the Internet.

The purpose for .hotel, is also to provide Hotels:

* A differentiated namespace focused on hotels

* Better, shorter names that are unavailable in the saturated Com/Net space

* Better Search engine rankings and discoverability.

The dependence of the Hotel industry on the Internet for bookings, promotion and sustenance also further substantiates the need for a ".Hotel" TLD. As per EuroStat(^6), the share of turnover generated via the Internet in the accommodation services sector rose from 3 % in 2004 to 14 % by 2008. As per a published paper on the 'E-Business Application" study on the Hospitality industry (Communications of the International Information Management Association, Volume 3 Issue 1), the hotel industry is certainly aware of this dependence on the internet. In 2002, over 51% of the total annual online bookings were earned through hotels' own websites (i.e., remaining 49% were through specialized online travel agencies).

For hotels, the internet is thus one of the primary sources of winning business. It's time the Internet gave them their own namespace to distinguish themselves from other businesses.

Our policies will allow restricted registration access to entities within the hotel industry only. We will back this policy with a well-defined Eligibility Restrictions Dispute Resolution Process (ERDRP) which allows us to rapidly take-down domain names that do not meet our eligibility criteria. It is our over-arching goal to develop .hotel as a clean, exclusive and high-quality name space.

Our mission, goals can be summarized as follows:

1.1 ENHANCE TRUST

To create a "trusted and secure" namespace for the hotel industry, and the users that seek them out through this medium.

1.2 ENHANCE SEARCHABILITY AND RECOGNITION

.hotel benefits the Registrants as well as the end users. End users will be able to find the website of a hotel easily amongst the sea of countless others in unrestricted gTLDs.

Entities within the hotel industry will be able to easily distinguish themselves by running their web presence on a .hotel domain name. The space will make them more visible, and more accessible.

1.3 ENHANCE REGISTRANT CHOICE

To create a namespace that provides hotels greater choice to represent themselves online in a manner they please. Due to the saturation and unrestricted nature of the existing gTLD space many have to opt for a name that does not best reflect them .hotel will provide legitimate Registrants a higher probability of obtaining their desired name

1.4 CREATE A CLEANER INTERNET SPACE

To create a cleaner internet experience for end users by implementing pioneering registration policies, content and usage policies, and abuse mitigation processes.

1.5 CREATE A STABLE AND RESILIENT INTERNET SPACE

To deliver a stable and resilient internet experience to registrants and end-users by going above and beyond the ICANN mandated SLAs and delivering 100% resolution uptime

External References:

* (^1)http://www.expedia.co.in/Hotels

* (^2) http://www.hrs.com/web3/showCmsPage.do;jsessionid=1E26D362CECE5BCC697B728C9FD20763.8-3?clientId=ZW5fVVNfTkVYVA--&cid=8-3&pageId=standard-01841

* (^3) http://www.icann.org/en/tlds/stld-apps-19mar04/travel.htm

* (^4) http://www.livemint.com/2011/11/07192833/Hospitality-industry-is-still.html?atype=tp

* (^5) http://www.ibef.org/download/Tourism_and_Hopitality50112.pdf

* (^6)

http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Hotel_and_accommodation_statistics

This completes our response to Q18(a).

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

1. GOAL OF .HOTEL

1.1 SPECIALTY

Our goal for .Hotel in terms of area of specialty is to be able to provide the Global Hotel Industry with a TLD that gives them a distinct identity on the web - their Global Home.

The .Hotel registry will open up a completely new space to the Hotel industry where they do not have to clamor for good domain name options, and where the opportunity to get their real estate on the internet is a lot simpler. A "Carlson.Hotel" will definitely have more branding value over "Carlsonhotels.com" – Shorter name, better SEO listing, and the .Hotel branding to go with it.

Our goal is to provide those associated with the Hotel industry with a differentiated space where they can build a distinct online identity, and can distinguish themselves from players from other industries.

1.2 SERVICE LEVELS

Our goal for .Hotel in terms of service levels is to go above and beyond the ICANN SLAs. ICANN provides for its expected SLA in Specification 10 in the Registry Agreement in the Applicant guidebook.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provides registry services for a number of TLDs including the .au ccTLD.

Our contract with ARI is attached to our response to Q46. This contract details the SLA we intend on achieving with this TLD. As can be seen in the contract we have exceeded the ICANN required SLA on every parameter.

Our response to Q34 and Q35 provides details on ARI's distributed anycast DNS network. ARI's DNS network provides for 16 geo distributed sites resulting in a very low resolution latency for end-users, amongst the lowest in the industry.

It is our objective to provide 100% uptime, a resilient global DNS infrastructure, and very low latency in terms of DNS resolution for this TLD

1.3 REPUTATION

Reputation of our TLD is of paramount importance to us. The reputation of our TLD directly relates to how end-users on the internet perceive our Registrants. We will ensure the highest reputation of .Hotel by ensuring the following –
* Maintaining a high quality bar with respect to Registrants in the TLD
* Well defined Acceptable usage and content policies
* Well defined dispute resolution mechanisms
* Ensuring Whois accuracy to support abuse mitigation
* Well defined and implemented abuse mitigation processes
* Well defined and implemented rights protection mechanisms
* Exceptional service levels

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice described in considerable detail in our response to Q28 and Q29. We also commit to extremely high service levels that go beyond the stipulated service levels in the applicant guidebook.

2. CONTRIBUTION OF .HOTEL TO THE NAMESPACE

2.1 CONTRIBUTION IN TERMS OF COMPETITION, DIFFERENTIATION, OR INNOVATION

Per ICANN's Bylaws as amended June 24, 2011, ICANN's core value number six is "Introducing and promoting competition in the registration of domain names where practicable and beneficial in the public interest."

As of today, no TLD truly represents the Hotel Industry. None of the TLDs such as .com, .net, .org, .biz, .mobi etc. mean anything even remotely associated with the Hotel Industry. Even though .Travel has been around for a while, and has an indirect association with the Hotel business, there hasn't been significant association made here with our target market. With the growing importance of the internet, all those associated with this industry deserve to have the ability to distinguish themselves from the other businesses and to go online with a TLD that truly represents who they are.

.Hotel will also allow Registrants in the Global Hotel Industry to differentiate themselves from the 200+ million domain names out there. As of now a Hotel domain name appears identical to any other domain name in a .gTLD (com) or .ccTLD extension (eg .in). The .Hotel registry's differentiation will be "The Internet home of the Global hotel industry". The domain names available with .hotel are precise and create identity for hotels, the hotel business and services, which today's saturated namespace does not offer room for. The .Hotel namespace will hence encourage existing Hotel Websites to move their business on to their differentiated namespace.

.Hotel will automatically lend value to any Hotel with an online presence. The .Hotel registry will aim to create value and presence such that a Hotel business with a .Hotel extension will automatically be more recognized as a Hotel brand, as opposed to a hotel with a generic extension for their website. Moreover, .Hotel will also enable Hotel owners to get better search result listings. A www.hilton.hotel is likely to get a high position at Google if you search for "Hilton hotel".

.Hotel will provide registrants the option to register more desirable and shorter names as opposed to names they would have otherwise registered in existing gTLDs due to the high saturation of the existing namespaces. By offering more fresh choice of names, we will also aspire to be the first choice gTLD for anyone who is setting up a Hotel Business.

* Our intent is to operate .Hotel with a focus on integrity and quality for the .Hotel brand. This entails running robust abuse mitigation programs and pioneering Rights Protection Mechanisms from initiation, which in our case not only meets ICANN's requirements, but extends significantly beyond it as described in our response to Q28 and Q29.

3. USER EXPERIENCE GOALS

.Hotel considers both its Registrants and the end-users that access .Hotel websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Hotel.

Registrants of .Hotel have an assurance of a scalable, resilient registry with 100% uptime, low latency, and exemplary security standards. Registrants will have the option to register the domain name of their choice, without much saturation of the namespace. Our registration policies and abuse mitigation policies ensure that Registrants will get advantages like higher recognition, better branding and more desirable, shorter names.

Our content and acceptable use policies and abuse mitigation processes ensure that end-users are benefited from a clean namespace. These are described in further detail in our response to Q28 and Q29.

4. REGISTRATION POLICIES IN SUPPORT OF GOALS

4.1 GENERAL NAMES

The goals of .Hotel are outlined in the sections above. These goals are supported by the following artifacts –
* Registration policies and processes
* Acceptable usage policies and content guidelines
* Abuse mitigation processes
* Rights protection mechanisms
* Dispute resolution polices

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice. The salient aspects of all of the above are described below -
* DotHotel Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (ResellerClub.com and BigRock.com) and Web Hosting companies. With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain name abuse mitigation and rights protection. Directi has been heralded as a white hat registrar and the undisputed leader with respect to abuse mitigation.

* Our Abuse and compliance processes will be run by the Directi Group
* We have an elaborate and detailed Accepted usage and content policy that covers over 11 macro forms of violations
* .Hotel will create a zero-tolerance reputation when it comes to abuse
* We have a defined SLA for responding to abuse complaints ensuring guaranteed turn-around time on any abuse complaint depending on its severity
* We will work closely with LEA and other security groups to mitigate abuse within TLD by providing them with special interfaces (eg searcheable whois) and interacting with them regularly in terms of knowledge sharing.
* Other abuse mitigation steps we undertake include profiling, blacklisting, proactive quality reviews, industry collaboration and information sharing, regular sampling, contractual enforcements and sanctions
* The protection of trademark rights is a core goal of .Hotel. .Hotel will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPMs to prevent abusive registrations and rapidly take-down abuse when it does occur.
* Standard RPMs such as Sunrise, Trademarks claims service, URS, UDRP, SDRP, PDDRP, ERDRP, SPOC etc are all provided for. Additional RPMs such as Optional Trademark declaration, profiling and blacklisting, proactive quality reviews, APWG Review and others will also be provided.

The above salient points barely scratch the surface in detailing the steps that .Hotel will take in order to build a reputation of operating a clean, secure and trusted namespace. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29

4.2. OTHER NAMES

* We will reserve the following classes of domain names, which will not be available to registrants via the Sunrise or subsequent periods:
** The reserved names required in Specification 5 of the new gTLD Registry Agreement.
** The geographic names required in Specification 5 of the new gTLD Registry Agreement. See our response to Question 22 ("Protection of Geographic Names") for details.
** The registry operator will reserve its own name and variations thereof, and registry operations names (such as nic.hotel, registry.hotel, and www.hotel), so that we can point them to our Web site. Reservation of the registry operator's names was standard in ICANN's past gTLD contracts.
** We will also reserve names related to ICANN and Internet standards bodies (iana.hotel, ietf.hotel, w3c.Hotel, etc.), for delegation of those names to the relevant organizations upon their request. Reservation of this type of names was standard in ICANN's past gTLD contracts. The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.
* We will reserve generic names which will be set aside for distribution via special mechanisms.

5. PROTECTING PRIVACY OF REGISTRANTS' OR USERS' INFORMATION

.Hotel is committed to providing a secure and trusted namespace to its Registrants and end-users. To that extent we will have several measures for protecting the privacy or confidential information of registrants or users -

* Our Whois service (web-based whois, port 43 whois and searchable whois) all have built in abuse prevention mechanisms to prevent unauthorized access, data mining, data scraping and any other abusive behavior. Details of this are provided in our response to Q26

* .Hotel will allow Registrants to use privacy protection services provided by their Registrars in the form of a Proxy whois service as long as they follow the guidelines stipulated within our response to Q28 to prevent any abuse of the same

* As per the requirements of the new gTLD Registry Agreement (Article 2.17), we shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data. (This data is basically the registrant and contact data required to be published in the WHOIS.)

* We will also require each registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. As the registry operator, we shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

* As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Q24, Q30 and Q38 we detail the security policies and procedures we will use to protect the registry system and the data contained there from unauthorized access and loss.

* As registry operator we impose certain operational standards for our registrars. In order gain

and maintain accreditation for our TLD, we require them to adhere to certain information technology policies designed to help protect registrant data. These include standards for access to the registry system. Please see our response to Q24, Q25 and Q30 for details.

* We offer a "registry lock" service, designed to help protect participating registrants' contact data from unauthorized modification, and against unauthorized domain transfers and deletions. Please see our response to Q27 for details.

* .Hotel implements DNSSEC at the zone which guarantees origin authentication of DNS data, authenticated denial of existence, and data integrity. This protects end-users from a man-in-the-middle attack protecting the privacy of data of end-users.

6. OUTREACH AND COMMUNICATIONS

* Considering the Hotel Industry is not confined to any particular region, our approach will be Global in nature. To achieve this, we will emphasize distribution channels internationally – not just in one or more focused regions.

* We will also engage in relevant PR and outreach programs as well as ensure appropriate publication of information on our website.

* We will also look to engage with some of the top Hotels worldwide – their usage of the .hotel extension will thereby lend credibility to and build awareness of the namespace.

* Our outreach efforts will thus be directed towards our target market in coordination with Registrar partners, to ensure greater adoption of the .Hotel TLD. One important method of outreach will involve co-marketing programs with these Registrar partners. We will also leverage Directi's existing channel of 65,000 Resellers, and its strategic relationships with other ICANN Accredited Registrars.

The communication and outreach will focus on –
* Education amongst the Hotel Industry
* Generating awareness of our Registration policies, Acceptable usage and content policies, Abuse mitigation processes and Rights protection mechanisms

This completes our response to Q18(b).

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

.Hotel considers both its Registrants and the end-users that access .Hotel websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Hotel. To that extent it is our goal to –
* Reduce ⁄ minimize any incremental costs ⁄ negative consequences imposed upon our users
* Increase ⁄ maximize the value added to our Registrants and end-users
* Ensure that the net effect of .Hotel on its users is that of positive value creation

In this response we explore how .Hotel achieves a net benefit for Registrants and End-users.

1. MINIMIZING COSTS

1.1 REGISTRANTS

It is our goal to provide Registrants of .Hotel incremental value and minimize any negative consequences and costs associated with .Hotel. We address this in the following manner

1.1.1 SUNRISE, TRADEMARK CLEARINGHOUSE (TMCH), RIGHTS PROTECTION MECHANISMS (RPMs)

Rights protection is a core goal of .Hotel. Our Right Protection mechanisms go significantly above and beyond the mandatory RPMs ensuring protection of trademark and IP rights of domain registrants and reducing the costs associated with rights protection for Registrants. Our elaborate RPMs are described in significant detail in our response to Q29. Some salient aspects of these are as follows –

* We offer a sunrise period to provide an opportunity for legitimate Registrants to block domain names in .Hotel before general availability begins, preventing unnecessary post-facto litigation

* We will integrate with the Trademark ClearingHouse in the manner prescribed to provide the

Trademarks claims service, so as to alert potential Registrants of any trademark violations prior to registration, as well as notify mark holders of potential mark violations

* We will provide SDRP, URS, UDRP, ERDRP and PDDRP reducing litigation costs by providing legitimate Registrants the opportunity to resolve disputes through standardized arbitration proceedings.

* Additionally we have pioneering RPMs like Optional Trademark Declaration, Profiling and Blacklisting, Proactive Quality assurance, APWG review etc – all intended to reduce rights violations and hence reduce costs for Registrants

The above salient points barely scratch the surface in detailing the steps that .Hotel will take in order to reduce costs of Registrants with respect to rights violations. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29.

1.1.2 MULTIPLE APPLICATIONS FOR A DOMAIN

All of the RPMs described in section 1.1.1 above ensure that applicants for domain names in .Hotel are legitimate right holders for the applied string.

During general availability domain names will be allocated on a first come first serve basis amongst applicants. During the initial registry launch periods of Sunrise and Landrush if multiple applications for the same domain name are received from applicants then the same will be distributed in the following manner –

* Incase of multiple sunrise applications for the same domain name, all applications will be validated against the TMCH for a valid trademark. Applications that do not qualify will be dropped.

* All remaining applications will be distributed through a fair auction.

1.1.3 COST BENEFITS FOR REGISTRANTS

The ICANN new gTLD program marks a historical event in the timeline of the Internet. It is an unprecedented event and one that will yield tremendous benefits for consumers. At this preliminary stage it is impossible to determine the true value consumers will derive from increase in competition and choice. However there is historical data to go by. Upon the launch of Domain Registrars and creation of competition amongst registrars, the Registrants benefited from reduced pricing.

With .Hotel our goal is to provide fair pricing for domains within .Hotel that reflect the value proposition derived by the Registrants of .Hotel. While we do not have any committed pricing plans as yet and the same will be determined during the launch process, we do anticipate providing promotional offers through the life of .Hotel for the purpose of customer acquisition. This is not too dissimilar from other gTLD registries currently in existence who offer ongoing promotional offers to their customer base.

1.1.4 PRICE ESCALATIONS

The ICANN new gTLD program is an unprecedented event and the actual nature of pricing pressures will only be determinable once several TLDs have successfully launched. At this preliminary stage it is impossible to commit to any pricing strategy on our part. We strongly believe that ultimately, the open market will determine the viability of pricing models and dictate pricing strategy for everyone. We intend to maintain the freedom to set pricing to accommodate for the existence of 100s of TLDs and business models and create a sustainable long term business model. Our goal is to provide fair pricing for domains within .Hotel that reflect the value proposition derived by the Registrants of .Hotel.

1.2 END USERS

It is our goal to provide end users of .Hotel incremental value and minimize any negative consequences and costs associated with .Hotel. We address this in the following manner

End-users bear a considerable amount of cost as a result of various forms of Internet abuse such as spam, malware, phishing, pharming, hacking, identity theft etc. Any TLD that implements policies and processes to create a clean namespace will result in a considerable reduction of these forms of abuse and hence a significant saving in terms of cost to consumers

.Hotel intends to set an example when it comes to abuse mitigation and preventing abuse within .Hotel. To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common

practice. These are detailed in our response to Q28. We strongly believe these practices will result in a significant reduction in online abuse and considerable savings for end users of .Hotel. We similarly hope to set an example for other TLDs and cooperate with the industry in creating a clean internet experience for internet users.

2. COST BENEFIT ANALYSIS

There has been considerable debate within the community concerning the cost benefit analysis of launching new gTLDs. We strongly believe that the launch of new gTLDs and our implementation of .Hotel will and add considerable value and result in a net positive effect on Registrants and end-users worldwide.

We recognize that there will be a post launch review of the New gTLD Program, from the perspective of assessing the relative costs and benefits achieved in the expanded gTLD space.

To this extent we would like to offer the following pointers concerning .Hotel as well as the general expansion of the new gTLD space in determining the net positive value generated for Registrants and end users –

* .Hotel will reduce overall cost for end-users in combating fraud and other forms of online abuse by implementing pioneering processes and anti-abuse policies as described in our response to Q28. Billions of dollars are spent worldwide combating various forms of fraud such as malware, phishing, spamming etc. Our abuse policies will result in overall reduction of these forms of abuses within .Hotel resulting in a considerable reduction in global costs spent towards combating these abuses. We also strongly believe that introduction of new gTLDs will result in increased competition which will drive significant innovation as well as competitive pressures for everyone in the industry to improve their abuse mitigation processes resulting in overall cost reduction for end-users

* The value of a Registrant getting the name they want is immeasurably larger than any costs resulting from expansion of the namespace. DotHotels Inc. is a subsidiary within the Directi Group which owns and operates several ICANN Accredited Registrars. Our stats show that 70% of the users who check for a .com domain name do not get their desired name. Until this launch of the new gTLD program there were very limited alternatives and none very viable/desirable for Registrants to choose from. .Hotel will expand the namespace thus providing a higher probability for new Registrants to obtain names they desire

* In general increased competition always results in pricing benefits for Registrants. .Hotel will provide additional options to new Registrants resulting in overall benefits to Registrants

* By virtue of registering a domain name within .Hotel, Registrants declare themselves to be associated with the Hotel industry. This adds considerable value in terms of searchability, SEO, creating trust, branding and a sense of belonging. As of now the only mechanism that exists for users to find a specific website are search engines. Search engines however do not classify the results in any manner to make it easier for users to determine which links are relevant to them with respect to their current search. .Hotel enables Registrants to standout amongst search results and allows end users to directly correlate as to whether a search result will likely be what they are looking for. This adds considerable value to Registrants who can be easily found now, and to end-users who will take lesser time to find specific sites.

This completes our response to Q18(c).

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.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes protection of geographic names as implemented by ARI.

1. PROTECTION OF GEOGRAPHIC NAMES

In accordance with Specification 5 of the New gTLD Registry Agreement, we will initially reserve all geographic names at the second level, and at all other levels within the TLD at which the registry operator provides for registrations.

ARI supports this requirement by using the following internationally recognised lists to develop a comprehensive master list of all geographic names that are initially reserved:

- 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 [http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm].

- 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].
- The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardisation of Geographical Names, Part III Names of Countries of the World. This lists the names of 193 independent States generally recognised by the international community in the language or languages used in an official capacity within each country and is current as of August 2006[http://unstats.un.org/unsd/geoinfo/ungegn/docs/pubs/UNGEGN%20tech%20ref%20manual_m87_combined.pdf].
- 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 standardisation of Geographical Names [http://unstats.un.org/unsd/geoinfo/UNGEGN/docs/9th-uncsgn-docs/econf/9th_UNCSGN_e-conf-98-89-add1.pdf].

Names on this reserved list in ARI's registry system are prevented from registration.

A corresponding list of geographic names will also be available to the public via our website, to inform Registrars and potential registrants of reserved names. The lists noted above, are regularly monitored for revisions, therefore the reserved list (both within the registry and publicly facing) will be continually updated to reflect any changes.

In addition to these requirements, ARI are able to support the wishes of the Governmental Advisory Council (GAC) or any individual Government in regard to the blocking of individual terms on a case by case basis. ARI's registry system allows such additions to be made by appropriately authorised staff, with no further system development changes required.

The following applies to all Domain Names contained within the registry's reserved list:
- Attempts to register listed Domain Names will be rejected.
- WhoIs queries for listed Domain Names will receive responses indicating their reserved status.
- Reserved geographic names will not appear in the TLD zone file.
- DNS queries for reserved domain names will result in an NXDOMAIN response.

2. PROCEDURES FOR RELEASE

We understand that if we wish to release the reserved names at a later date, this will require agreement from the relevant government(s) or review by the GAC, and subsequent approval from ICANN.

This completes our response to Q22.

Registry Services

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

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes the Registry Services for our TLD, as provided by ARI.

1. INTRODUCTION

ARI's Managed TLD Registry Service is a complete offering, providing all of the required Registry services. What follows is a description of each of those services.

2. REGISTRY SERVICES

The following sections describe the registry services provided. Each of these services has, where required, been designed to take into account the requirements of consensus policies as documented here:
[http://www.icann.org/en/resources/Registrars/consensus-policies]

2.1 RECEIPT OF DATA FROM REGISTRARS

The day-to-day functions of the Registry, as perceived by Internet users, involves the receipt of data from Registrars and making the necessary changes to the SRS database. Functionality such as

the creation, renewal and deletion of domains by Registrars, on behalf of Registrants, is provided by two separate systems:

* An open protocol -based provisioning system commonly used by Registrars with automated domain management functionality within their own systems.
* A dedicated website providing the same functionality for user interaction.

Registrants (or prospective Registrants) who wish to manage their existing domains or credentials, register new domains or delete their domains will have their requests carried out by Registrars using one of the two systems described below.

ARI operates Extensible Provisioning Protocol (EPP) server software and distributes applicable toolkits to facilitate the receipt of data from Registrars in a common format. EPP offers a common protocol for Registrars to interact with SRS data and is favoured for automating such interaction in the Registrar's systems. In addition to the EPP server, Registrars have the ability to use a web -based management interface (SRS Web Interface), which provides functions equivalent to the EPP server functionality.

2.1.1 EPP

The EPP software allows Registrars to communicate with the SRS using a standard protocol. The EPP server software is compliant with all appropriate RFCs and will be updated to comply with any relevant new RFCs or other new standards, as and when they are finalised. All standard EPP operations on SRS objects are supported.

Specifically, the EPP service complies with the following standards:

* 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 the Extensible Provisioning Protocol (EPP).
* RFC 3915 Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP).
* Extensions to ARI's EPP service comply with RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP).

2.1.1.1 SECURITY FOR EPP SERVICE

To avoid abuse and to mitigate potential fraudulent operations, the EPP server software uses a number of security mechanisms that restrict the source of incoming connections and prescribe the authentication and authorisation of the client. Connections are further managed by command rate limiting and are restricted to only a certain number for each Registrar, to help reduce unwanted fraudulent and other activities. Additionally, secure communication to the EPP interface is required, lowering the likelihood of the authentication mechanisms being compromised.

The EPP server has restrictions on the operations it is permitted to make to the data within the Registry database. Except as allowed by the EPP protocol, the EPP server cannot update the credentials used by Registrars for access to the SRS. These credentials include those used by Registrars to login to ARI's SRS Web Interface and the EPP service.

Secure communication to the EPP server is achieved via the encryption of EPP sessions. The Registry system and associated toolkits support AES 128 and 256 via TLS.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

The Production and Operational Testing and Evaluation (OTE) EPP service is protected behind a secure firewall that only accepts connections from registered IP addresses. Registrars are required to supply host IP addresses that they intend to use to access the EPP service.

Certificates are used for encrypted communications with the Registry. Registrars require a valid public⁄private key pair signed by the ARI CA to verify authenticity. These certificates are used to establish a TLS secure session between client and server.

EPP contains credential elements in its specification which are used as an additional layer of authentication. In accordance with the EPP specification, the server does not allow client sessions to carry out any operations until credentials are verified.

The EPP server software combines the authentication and authorisation elements described above to ensure the various credentials supplied are associated with the same identity. This verification requires that:

* The username must match the common name in the digital certificate.
* The certificate must be presented from a source IP listed against the Registrar whose common

name appears in the certificate.
* The username and password must match the user name and password listed against the Registrar's account with that source IP address.

To manage normal operations and prevent an accidental or intentional Denial of Service, the EPP server can be configured to rate limit activities by individual Registrars.
Further details are provided for in Q24 and Q25.

2.1.1.2 STABILITY CONSIDERATIONS

The measures that restrict Registrars to a limit of connections and operations for security purposes also serve to keep the SRS and the EPP server within an acceptable performance and resource utilisation band. Therefore, scaling the service is an almost linear calculation based on well-defined parameters.

The EPP server offers consistent information between Registrars and the SRS Web Interface. The relevant pieces of this information are replicated to the DNS within seconds of alteration, thus ensuring that a strong consistency between the SRS and DNS is maintained at all times.

2.1.2 SRS WEB INTERFACE

The Registry SRS Web Interface offers Registrars an alternative SRS interaction mechanism to the EPP server. Available over HTTPS, this interface can be used to carry out all operations which would otherwise occur via EPP, as well as many others. Registrars can use the SRS Web Interface, the EPP server interface or both — with no loss of consistency within the SRS.

2.1.2.1 SECURITY AND CONSISTENCY CONSIDERATIONS FOR SRS WEB INTERFACE

The SRS Web Interface contains measures to prevent abuse and to mitigate fraudulent operations. By restricting access, providing user level authentication and authorisation, and protecting the communications channel, the application limits both the opportunity and scope of security compromise.

Registrars are able to create individual users that are associated with their Registrar account. By allocating the specific operations each user can access, Registrars have full control over how their individual staff members interact with the SRS. Users can be audited to identify which operations were conducted and to which objects those operations were applied.

A secure connection is required before credentials are exchanged and once authenticated. On login, any existing user sessions are invalidated and a new session is generated, thereby mitigating session-fixation attacks and reducing possibilities that sessions could be compromised.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

2.1.3 SECURING AND MAINTAINING CONSISTENCY OF REGISTRY-REGISTRAR INTERACTION SYSTEMS

ARI ensures all systems through which Registrars interact with the SRS remain consistent with each other and apply the same security rules. Additionally, ARI also ensures that operations on SRS objects are restricted to the appropriate entity. For example:

* In order to initiate a transfer a Registrar must provide the associated domain password (authinfo) which will only be known by the Registrant and the current sponsoring Registrar.
* Only sponsoring Registrars are permitted to update Registry objects.
All operations conducted by Registrars on SRS objects are auditable and are identifiable to the specific Registrar's user account, IP address and the time of the operation.

2.2 DISSEMINATE 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. ARI will 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 those when:
* 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.

2.2.1 COMMUNICATION POLICY

ARI maintains 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 time frame, 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 down time. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

2.2.2 SECURITY AND STABILITY CONSIDERATIONS

ARI restricts zone server status communication to Registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, ARI ensures 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 organisations 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.

ARI will fully comply with the processes and procedures dictated by the Centralised 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, ARI updates the zone file on the TLD zone servers using software compliant with RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE)) and RFC 2845 (Secret Key Transaction Authentication for DNS (TSIG)).

This updating process follows 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 ARI’s 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 protocols for dynamic update are robust and mature, as is their implementation in DNS software. The protocols’ mechanisms for ensuring consistency within and between updates are fully implemented in ARI’s 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. ARI has used this method for updating zone files in all its TLDs including the .au ccTLD, pioneering this method during its inception in 2002. Mechanisms separate to RFC 2136-compliant transfer processes exist; to check and ensure domain information is consistent with the SRS on each TLD zone server within 10 minutes of a change.

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 recognised by ARI 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 centres 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, authorisation 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 CONTACT OR OTHER INFORMATION

Registries are required to provide a mechanism to identify the relevant contact information for a domain. The traditional method of delivering this is via the Whois service, a plain text protocol commonly accessible on TCP port 43. ARI also provides the same functionality to users via a web -based Whois service. Functionality remains the same with the web -based service, which only requires a user to have an Internet browser.

Using the Whois service, in either of its forms, allows a user to query for domain -related information. Users can query for domain details, contact details, nameserver details or Registrar details.

A Whois service, which complies with RFC 3912, is provided to disseminate contact and other information related to a domain within the TLD zone.

2.6.1 SECURITY AND STABILITY CONSIDERATIONS

ARI ensures the service is available and accurate for Internet users, while limiting the opportunity for its malicious use. Many reputation and anti-abuse services rely on the availability and accuracy of the Whois service, However the potential for abuse of the Whois service exists.

Therefore, certain restrictions are made to the access of Whois services, the nature of which depend on the delivery method – either web -based or the traditional text -based port 43 service. In all cases, there has been careful consideration given to the benefits of Whois to the Internet community, as well as the potential harm to Registrants - as individuals and a group - with regard to Whois access restrictions.

The Whois service presents data from the Registry Database in real time. However this access is restricted to reading the appropriate data only. The Whois service does not have the ability to alter data or to access data not related to the Whois service. The access limitations placed on the Whois services prevent any deliberate or incidental denial of service that might impact other Registry Services.

Restrictions placed on accessing Whois services do not affect legitimate use. All restrictions are designed to target abusive volume users and to provide legitimate users with a fast and available service. ARI has the ability to 'whitelist' legitimate bulk users of Whois, to ensure they are not

impacted by standard volume restrictions.

The data presentation format is consistent with the canonical representation of equivalent fields, as defined in the EPP specifications and ICANN agreement.

2.6.1.1 PORT 43 WHOIS

A port 43 -based Whois service complying with RFC 3912 is provided and will be updated to meet any other relevant standards or best practice guidelines related to the operation of a Whois service. While the text -based service can support thousands of simultaneous queries, it has dynamic limits on queries per IP address to restrict data mining efforts. In the event of identified malicious use of the service, access from a single IP address or address ranges can be limited or blocked.

2.6.1.2 WEB -BASED WHOIS

ARI's web -based Whois service provides information consistent with that contained within the SRS. The web -based Whois service contains an Image Verification Check (IVC) and query limits per IP address. These restrictions strike a balance between acceptable public usage and abusive use or data mining. The web -based Whois service can blacklist IP addresses or ranges to prevent abusive use of the service.

2.6.1.3 SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service for the identification of domain names having similar registration data. This service, deployed as a web-interface alongside the SRS Web Interface, is restricted to pre-authorised clients.

The service is made available to authorized third parties. ARI will perform relevant background checks on a user before providing them with access to the searchable whois. The user will be required to change their password on first successful login, and every 6 months thereafter. Clients that have not used the service in a 3-month period will have their access revoked. ARI will periodically review the information submitted by the client to ensure that contact and usage information is up to date.

Access is logged and monitored to protect against abuse of this service. All searches are logged with the client and timestamp of the request. IP address, port, and browser information is collected in the event that this information is required to assist in identifying the user. The use of HTTPS is enforced for the entire service to prevent exposure of the information from client -side or middle-box caches.

ARI will conduct periodic audits of query logs to identify usage patterns and identify potential occurrences of data mining. Usage patterns will be matched back to the client's specified reason for use. The client may be suspended from use of the service if ARI believes that abuse is occurring.

Further details on this service are described in the answer to Question 262.7 IDNs—Internationalised Domain Names

An Internationalised Domain Name (IDN) allows registrants to register domains in their native language and have it display correctly in IDN aware software. This includes allowing a language to be read in the manner that would be common for its readers. For example, an Arabic domain would be presented right to left for an Arabic IDN aware browser.
The inclusion of IDNs into the TLD zones is supported by ARI. All the Registry services, such as the EPP service, SRS Web Interface and RDPS (web and port 43), support IDNs. However there are some stability and security considerations related to IDNs which fall outside the general considerations applicable individually to those services.

2.7.1 STABILITY CONSIDERATIONS SPECIFIC TO IDN

To avoid the intentional or accidental registration of visually similar chars, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

2.7.1.1 PREVENT CROSS LANGUAGE REGISTRATIONS

Domains registered within a particular language are restricted to only the chars of that language. This avoids the use of visually similar chars 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.

2.7.1.2 INTER-LANGUAGE AND INTRA-LANGUAGE VARIANTS TO PREVENT SIMILAR REGISTRATIONS

ARI restricts child domains to a specific language and prevents registrations 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. Recommendation 26 calls for DNSSEC deployment at each zone and subsequent sub-zones at Registry, Registrar and Registrant level. Our compliance wrt the same is detailed in Q43.

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 RECEIPT OF PUBLIC KEYS FROM REGISTRARS

The public key for a child domain is received by ARI from the Registrar via either the EPP or SRS Web Interface. ARI uses an SHA-256 digest to generate the DS Resource Record (RR) for inclusion into the zone file.

2.8.1.3 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. 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, ARI 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, ARI 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.

This completes our response to Q23.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q24 – ARI Background & Roles.pdf'. This response describes the SRS as implemented by ARI.

1. INTRODUCTION

ARI has demonstrated delivery of an SRS with exceptional availability, performance and reliability. ARI's SRS has successfully supported a large group of Registrars for ASCII and IDN based TLDs. ARI's SRS meets the following requirements:

* Resilient to wide range of security & availability threats
* Consistently exceeds performance & availability SLAs
* Allows capacity increase with minimal impact to service
* Provides fair & equitable provisioning for all Registrars

2. CAPACITY

ARI's SRS infrastructure was built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [http://www.icann.org/en/resources/registries/reports] we know there is:

 * An average of 70 SRS TPS per domain, per month; and
 * A ratio of 3 query to 2 transform txs

For a Registry with 20M domains this indicates an expected monthly transaction volume of 1,400M txs (840M query and 560M transforms).

Through conservative comparison of .au registry numbers and the .net RFP response - specifically http://archive.icann.org/en/tlds/net-rfp/applications/sentan.htm we also know:

 * The peak daily txs is 6% of the monthly total (.au:6%, .net: 5%)
 * The peak 5 min txs is 5% of the peak daily (.au and .net: 5%)

Hence for 20M domains we expect a peak EPP tx rate of 14,000 TPS (5,600 transform TPS and 8,400 query TPS)
Through conservative statistical analysis of the .au registry we additionally know:

 * The avg no. of contacts/domain is 3.76 (overall not assigned)
 * The avg no. of hosts/domain is 2.28 (overall not assigned)

This translates into a requirement to store 75.2M contacts and 45.6M hosts.
Finally through real world observations of the .au registry, which has a comprehensive web interface when compared to those offered by current gTLD registries, we know that there is an avg of 0.5 HTTP requests/sec to the SRS web interface per registrar. We also know that this behaviour is reasonably flat. To support an estimated 1000 Registrars, would require into a HTTP request load of 500 requests/second.

For perspective on the conservativeness of this, the following was taken from data in the May 2011 ICANN reports referenced above:

* .info: ~7.8M domain names peaks at ~1,400 TPS (projected peak TPS of ~3,600 with 20M)

* .com: ~98M domain names peaks at ~41,000 TPS (projected peak TPS of ~8,300 TPS with 20M)

* .org: ~9.3M domain names, peaks at ~1,400 TPS (projected peak TPS of ~3,100 with 20M)

After performing this analysis the projected TPS for .com was still the largest value seen. ARI's estimated value of 14,000 TPS for a registry with 20M Domains is roughly twice that of the .com projected peak of ~8300 TPS.

ARI benchmarked their SRS infrastructure and used the results to calculate the required computing resources for each of the tiers within the SRS architecture; allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server in the architecture, and the network bandwidth & and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions, and headroom. Despite doubling numbers, effective estimated capacity is still reported as 20M. The technical resource allocations are explored in Q32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.

.Hotel is projected to reach 26,715 domains at its peak volume and will generate 18.7 EPP TPS. This will consume 0.13% of the resources of the SRS infrastructure. As is evident ARI's SRS can easily accommodate this TLD's growth plans. See attachment 'Q24_Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's SRS infrastructure will be only 60% utilized in 2014. The SRS infrastructure capacity can also be easily scaled as described in Q32

3. SRS ARCHITECTURE

ARI's SRS has the following major components:
* Network Infrastructure
* EPP Application Servers
* SRS Web Interface Application Servers
* SRS Database

Attachment 'Q24 – SRS.pdf' shows the SRS systems architecture and data flows. Detail on this architecture is in our response to Q32. ARI provides two distinct interfaces to the SRS: EPP and SRS Web. Registrar SRS traffic enters the ARI network via the redundant Internet link and passes (via the firewall) to the relevant application server for the requested service (EPP or SRS Web). ARI's EPP interface sustains high volume and throughput domain provisioning transactions for a large number of concurrent Registrar connections. ARI's SRS Web interface provides an alternative to EPP and provides features additional to those provided by the EPP interface.

3.1 EPP

ARI's EPP application server is based on EPP as defined in RFCs 5730 – 5734. Registrars send XML based transactions to a load balanced EPP interface which forwards to one of the EPP application servers. The EPP application server then processes the XML and converts the request into database calls that retrieve or modify registry objects in the SRS database. The EPP application server tier comprises of 3 independent servers with dedicated connections to the Registry database. Failure of any one of these servers will cause Registrar connections to automatically re-establish with one of the remaining servers. All EPP servers accept EPP both IPv4 & IPv6.

3.2 SRS WEB

The SRS Web application server is a Java web application. Registrars connect via the load balancer to a secure HTTPS listener running on the web servers. The SRS web application converts HTTPS requests into database calls which query or update objects in the SRS database. The SRS Web application server tier consists of 2 independent servers that connect to the database via JDBC. If one of these servers is unavailable the load balancer re-routes requests to the surviving server. These servers accept both IPv4 & IPv6.

3.3 SRS DATABASE

The SRS database provides persistent storage for domains and supporting objects. It offers a secure way of storing and retrieving objects provisioned within the SRS and is built on the Oracle 11g Enterprise Edition RDBMS. The SRS Database tier consists of four servers clustered using

Oracle Real Application Clusters (RAC). In the event of failure of a database server, RAC will transparently transition its client connections to a surviving database host.

The SRS database is stored on a storage area network concurrently accessed by all of the database servers which supports N+N redundancy. The SAN consists of 2 switches, 2o control enclosures (each with dual controllers), and 2 expansion enclosures per control enclosure. Each database server host is configured with two 4-port Fibre Channel Host Bus Adaptors (HBAs). Each HBA has 2 SAN fabric connections, one to each SAN switch — providing a total of 4 fabric connections per database server.

Each SAN switch has dual redundant connections to each controller in each Control Enclosure. All disks under the control of a Control Enclosure are configured in a highly resilient RAID 10 array. The Storwize V7000 uses SAN mirroring technology to duplicate data across Control Enclosures. This SAN design provides protection against failure of any component within the Storage Area Network including complete loss of a Control Enclosure and associated expansion enclosures.

3.4 NUMBER OF SERVERS

EPP Servers – The EPP cluster consists of 3 EPP servers that can more than handle the anticipated 20M. .Hotel will utilize 0.13% of this at its peak volume. As the utilization increases ARI will add additional EPP servers ensuring the total utilization doesn’t exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

SRS Web Servers – The SRS Web cluster consists of 2 SRS Web servers that can more than handle the anticipated 20M. .Hotel will utilize 0.13% of this at its peak volume. As the utilization increases ARI will add additional SRS Web servers ensuring total utilization doesn’t exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

SRS DB Servers – The SRS DB cluster consists of 4 SRS DB servers that can more than handle the anticipated 20M. .Hotel will utilize 0.13% of this at its peak volume. As the utilization increases ARI will add additional SRS DB servers ensuring total utilization doesn’t exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

3.5 SRS SECURITY

ARI adopts a multi-layered security solution to protect the SRS. An industry leading firewall is deployed behind the edge router and is configured to only allow traffic on the minimum required ports and protocols. Access to the ARI EPP service is restricted to a list of known Registrar IPs.

An Intrusion Detection device is in-line with the firewall to monitor and detect suspicious activity.

All servers are configured with restrictive host based firewalls, intrusion detection, and SELinux. Direct root access to these servers is disabled and all access is audited and logged centrally.

The SRS database is secured by removal of non-essential features and accounts, and ensuring all remaining accounts have strong passwords. All database accounts are assigned the minimum privileges required to execute their business function.

All operating system, database, and network device accounts are subject to strict password management controls such as validity & complexity requirements.

Registrar access to the SRS via EPP or the Web interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows:

* Registrar’s source IP address must be allowed by the front-end firewalls. This source IP address is received from the Registrar via a secure communication channel from within the SRS Web interface;
* Registrar must use a digital certificate provided by ARI;
* Registrar must use authentication credentials that are provided by to the Registrar via encrypted email.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as ‘Acceptable’ till ‘2031 and beyond’ by NIST Special Publication 800-57.

3.6 SRS HIGH AVAILABILITY

SRS availability is of paramount importance. Downtime is eliminated or minimised where possible. The infrastructure contains no single points of failure. N+1 redundancy is used as a minimum, which not only protects against unplanned downtime but also allows ARI to execute maintenance without impacting service.

Redundancy is provided in the network with hot standby devices & multiple links between devices. Failure of any networking component is transparent to Registrar connections.

N+N redundancy is provided in the EPP and SRS Web application server tiers by the deployment of multiple independent servers grouped together as part of a load -balancing scheme. If a server fails the load balancer routes requests to the remaining servers.

N+N redundancy is provided in the database tier by the use of Oracle Real Application Cluster technology. This delivers active⁄active clustering via shared storage. This insulates Registrars from database server failure.

Complete SRS site failure is mitigated by the maintenance of a remote standby site — a duplicate of the primary site ready to be the primary if required.

The standby site database is replicated using real time transaction replication from the main database using Oracle Data Guard physical standby. If required the Data Guard database can be activated quickly and service resumes at the standby site.

3.7 SRS SCALABILITY

ARI's SRS scales efficiently. At the application server level, additional computing resource can be brought on-line rapidly by deploying a new server online. During benchmarking this has shown near linear.

The database can be scaled horizontally by adding a new cluster node into the RAC cluster online. This can be achieved without disruption to connections. The SRS has demonstrated over 80% scaling at the database level, but due to the distributed locking nature of Oracle RAC, returns are expected to diminish as the number of servers approaches double digits. To combat this ARI ensures that when the cluster is 'scaled' more powerful server equipment is added rather than that equal to the current members. Capacity can be added to the SAN at any time without downtime increasing storage and IOPs.

Additional capacity can be added to the SAN at anytime without downtime. This would result in increasing storage and IOPs.

3.8 SRS INTER-OPERABILITY AND DATA SYNCHRONISATION

The SRS interfaces with a number of related Registry systems as part of normal operations.

3.8.1 DNS UPDATE

Changes made in the SRS are propagated to the DNS via an ARI proprietary DNS Update process. This process runs on the 'hidden' primary master nameserver and waits on a queue. It is notified when the business logic inserts changes into the queue for processing. The DNS Update process reads these queue entries and converts them into DNS update (RFC2136) commands that are sent to the nameserver. The process of synchronising changes to SRS data to the DNS occurs in real-time.

3.8.2 WHOIS

The provisioned data supporting the SRS satisfies Whois queries. Thus the Whois and SRS share data sets and the Whois is instantaneously updated. Under normal operating conditions the Whois service is provided by the infrastructure at the secondary site in order to segregate the load and protect SRS from Whois demand (and vice versa). Whois queries that hit the standby site will query data stored in the standby database — maintained in near real-time using Oracle Active Data Guard. If complete site failure occurs Whois and SRS can temporarily share the same operations centre at the same site (capacity numbers are calculated for this).

3.8.3 ESCROW

A daily Escrow extract process executes on the database server via a dedicated database account with restricted read-only access. The results are then transferred to the local Escrow Communications server by SSH.

4. OPERATIONAL PLAN

ARI follow defined policies/procedures that have developed over time by running critical Registry systems. Some principals captured by these are:

* Conduct all changes & upgrades under strict and well-practised change control procedures
* test, test and test again
* Maintain Staging environments as close as possible to production infrastructure/configuration
* Eliminate all single points of failure
* Conduct regular security reviews & audits
* Maintain team knowledge & experience via skills transfer/training
* Replace hardware when no longer supported by vendor
* Maintain spare hardware for all critical components
* Execute regular restore tests of all backups
* Conduct regular capacity planning exercises
* Monitor everything from multiple places but ensure monitoring is not 'chatty'
* Employ best of breed hardware & software products & frameworks (such as ITIL, ISO27001 and Prince2)
* Maintain two distinct OT&E environments to support pre*production testing for Registrars

5. DESCRIPTION OF SLA, RELIABILITY & COMPLIANCE

ARI's SRS adheres to and goes beyond the scope of Specification 6 and Specification 10 of the Registry Agreement

ARI's EPP service is XML compliant and XML Namespace aware. It complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts & contacts are compliant with RFC 5731, 5732 & 5733 respectively. The transport over TCP is compliant with RFC5734. The service also complies with official extensions to support DNSSEC, RFC5910, & Redemption Grace Period, RFC 3915.
ARI's SRS is sized to sustain a peak transaction rate of 14,000 TPS while meeting strict internal Service Level Agreements (SLAs). The monthly -based SLAs below are more stringent than those in Specification 10 (Section 2).
EPP Service Availability: 100%
EPP Session Command Round Trip Time (RTT): 〈=1000ms for 95% of commands
EPP Query Command Round Trip Time (RTT): 〈=500ms for 95% of commands
EPP Transform Command Round Trip Time (RTT): 〈=1000ms for 95% of commands
SRS Web Interface Service Availability: 99.9%
ARI measures the elapsed time of every query, transform and session EPP transaction, and calculate the percentage of commands that fall within SLA on a periodic basis. If percentage value falls below configured thresholds on-call personnel are alerted.
SRS availability is measured by ARI's monitoring system which polls both the EPP and SRS Web services status. These checks are implemented as full end to end monitoring scripts that mimic user interaction, providing a true representation of availability. These 'scripts' are executed from external locations on the Internet.

6. RESOURCES

This function will be performed by ARI. ARI staff are industry leading experts in domain name registries with the experience and knowledge to deliver outstanding SRS performance.

The SRS is designed, built, operated and supported by the following ARI departments:

* Products and Consulting team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q24 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Hotel projects 26,715 domains, 0.05% of these resources are allocated to this TLD. See attachment 'Q24_Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

7. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q24.

25. Extensible Provisioning Protocol (EPP)

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q25 - ARI Background & Roles.pdf'. This response describes the Extensible Provisioning Protocol (EPP) interface as implemented by ARI.

1. INTRODUCTION

ARI's EPP service is XML compliant and XML Namespace aware. The service complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts and contacts are compliant with RFC5731-3 respectively. The transport over TCP is implemented in compliance with RFC5734. The service also complies with the official extensions to support DNSSEC, RFC5910 and Redemption Grace Period, RFC3915. ARI implemented EPP draft version 0.6 in 2002, then migrated to EPP RFC 1.0 on its publishing in 2004. The system has operated live since 2002 in the .au ccTLD. Descriptions in this response follow the terminology used in the EPP RFCs. when referring to the software involved in the process, ARI's EPP interface is called the server, and the software used by Registrars is called the client.

2. TRANSPORT LAYER

The ARI EPP service implements the RFC5734 – EPP Transport over TCP. Connections are allowed using TLSv1 encryption, optionally supporting SSLv2 Hello for compatibility with legacy clients. AES cipher suites for TLS as described in RFC3268 are the only ones allowed.

2.1 AUTHENTICATION

Registrar access to the EPP interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows. Registrars must:

* Present a certificate, during TLS negotiation, signed by the ARI Certificate Authority (CA). The server returns a certificate also signed by the ARI CA. Not presenting a valid certificate results in session termination. ARI requires that the Common Name in the subject field of the certificate identifies the Registrar.

* Originate connections from an IP address that is known to be assigned to the Registrar with that Common Name.
** Registrar must use authentication credentials provided to the Registrar via encrypted email

* Registrars aren't able to exceed a fixed number of concurrent connections. The connection limit is prearranged and designed to prevent abuse of Registrars' systems from affecting the Registry. The limit is set to reasonable levels for each Registrar, but can be increased to ensure legitimate traffic is unaffected. If any of the above conditions aren't met the connection is terminated.

All communication between the Registrars and the EPP service is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

2.2 CONNECTION CLOSE

The server may close the connection as a result of a logout, an error where the state of the connection is indeterminate, or after a timeout. Timeout occurs where no complete EPP message is received on the connection for 10 minutes.

3. EPP PROTOCOL

This section describes the interface relating to the EPP protocol described in RFC5730. This includes session management, poll message functionality and Object mappings for domains, hosts and contacts.

3.1 SESSION MANAGEMENT

Session management refers to login and logout commands, used to authenticate and end a session with the SRS. The Login command is used to establish a session between the client and the server. This command succeeds when:
- The username supplied matches the Common Name in the digital certificate used in establishing the TLS session.
- The provided password is valid for the user.
- The user's access to the system isn't suspended.
The Logout command is used to end an active session. On processing a logout the server closes the underlying connection. The Hello command can be used as a session keep-alive mechanism.

3.2 SERVICE MESSAGES

Offline notifications pertaining to certain events are stored in a queue. The client is responsible for polling this queue for new messages and to acknowledge read messages. Messages include notification about server modification of sponsored objects, transfer operations, and balance thresholds.

4. EPP OBJECT MAPPINGS

This section covers the interface for the 3 core EPP objects; domain, host and contact objects, as per RFC5731, 5732, & 5733 respectively.

The EPP domain, contact and host object mapping describes an interface for the check, info, create, delete, renew (domain only), transfer (domain & contact only) and update commands. For domain objects The server doesn't support the use of host attributes as described by RFC5731, but rather uses host objects as described by RFC5731 and RFC5732. Details of each command are:.

* Check command: checks availability of 1 or more domain, contact or host objects in the SRS. Domain names will be shown as unavailable if in use, invalid or reserved, other objects will be unavailable if in use or invalid.

* info command: retrieves the information of an object provisioned in the SRS. Full information is returned to the sponsoring client or any client that provides authorisation information for the object. Non-sponsoring clients are returned partial information (no more than is available in the WhoIs).

* Create command: provisions objects in the SRS. To ascertain whether an object is available for provisioning, the same rules for the check command apply.

* Delete command: begins the process of removing an object from the SRS. Domain names transition into the redemption period and any applicable grace periods are applied. domain names within the Add Grace Period are purged immediately. All other objects are purged immediately if they are not linked.

* Renew command (domain only): extends the registration period of a domain name. The renewal period must be between 1 to 10 years inclusive and the current remaining registration period, plus the amount requested in the renewal mustn't exceed 10 years.

* Transfer command (domain and contact only): provides several operations for the management of the transfer of object sponsorship between clients. clients that provide correct authorisation information for the object can request transfers. Domain names may be rejected from transfer within 60 days of creation or last transfer. The requesting client may cancel the transfer, or the sponsoring client may reject or approve the transfer. Both the gaining and losing clients may query the status of the current pending or last completed transfer.

* Update command: updates authorisation information, delegation information (domains), and registration data pertaining to an object.

5. NON-PROPRIETARY EPP MAPPINGS

ARI's EPP service implements 2 non-proprietary EPP mappings, to support the required domain name lifecycle and to provide & manage DNSSEC information. The relevant schema documents aren't provided as they are published as RFCs in the RFC repository.

5.1 GRACE PERIOD MAPPING

The Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (as per RFC 3915) is used to support the domain name lifecycle as per existing TLDs.The update command is extended by the restore command to facilitate the restoration of previously deleted domains in the

redemption period. This command defines 2 operations, request & report, described here:

* Request operation: requests the restoration of a domain.

* Report operation: completes the restoration by specifying the information supporting the restoration of the domain. The restore report must include a copy of the Whois information at both the time the domain was deleted & restored, including the restore reason.

5.2 DNSSEC MAPPING

The Domain Name System (DNS) Security Extensions Mapping for EPP, as per RFC5910, is used to support the provisioning of DNS Security Extensions. ARI requires clients use the Key Data Interface. Clients may associate a maximum of 4 keys per domain. The Registry system generates the corresponding DS data using the SHA-256 digest algorithm for the domain and any active variant domains.

ARI is aware of issues DNSSEC causes when transferring DNS providers – a transfer of Registrar usually means a change in DNS provider. DNSSEC key data won't be removed from the SRS or the DNS if a transfer occurs. It is the responsibility of and requires the cooperation of the Registrant, Registrars, and DNS providers, to provide a seamless transition. ARI observes progress with this issue and implements industry agreed solutions as available. DNSSEC information is included in info responses when the secDNS namespace in login.

6. PROPRIETARY MAPPING

The Registry system supports 3 additional EPP extensions where no published standard for the required functionality exists. Developed to conform to the requirements specified in RFC3735, these extensions include the provisioning of Internationalised Domain Names and domain name variants, and the association of arbitrary data with a domain name. These 3 extensions are introduced below, and further described in the attached schema documentation.

6.1 INTERNATIONALISED DOMAIN NAMES

ARI has developed an extension to facilitate the registration and management of Internationalised Domain Names as per RFCs 5890-5893 (collectively known as the IDNA 2008 protocol). This extension extends the domain create command and the info response.
The create command is extended to capture the language table identifier that identifies the corresponding IDN language table for the domain name. Additionally the extension requires the Unicode form to avoid an inconsistency with DNS-form, as per RFC 5891.

The domain info command is extended to identify the language tag and Unicode form provided in the initial create command. This information is disclosed to all querying clients that provided the extension namespace at login. This extension is documented in the attachment 'Q25 – idnadomain-1.0.pdf'.

6.2 VARIANT

ARI has developed an extension to facilitate the management of Domain Name variants. This extension extends the domain update command and the domain create and info responses. The domain update command is extended to allow the addition (activation) and removal (de-activation) of domain name variants subject to registry operator policy.

The domain create and info responses are extended to return the list of activated domain name variants. This information is disclosed to all querying clients that provided the extension namespace at login. The extension is documented in the attachment 'Q25 – variant-1.1.pdf'.

6.3 KEY-VALUE

ARI has developed an extension to facilitate the transport of arbitrary data between clients and the SRS without the need for developing EPP Extensions for each specific use-case. This extension extends the domain create and domain update transform commands and the domain info query command. This extension is documented in the attachment 'Q25 – kv-1.0.pdf'.

7. ADDITIONAL SECURITY

The Registry system provides additional mechanisms to support a robust interface. The use of command rate limiting enables the Registry to respond to and withstand erroneous volumes of commands, while a user permission model provides fine-grained access to the EPP interface. These 2 mechanisms are described below.

7.1 RATE LIMITING

The Registry system supports command and global rate limits using a token-bucket algorithm. Limits apply to each connection to ensure fair and equitable use by all. Clients that exceed limits receive a command failed response message indicating breach of the limit.

7.2 USER PERMISSION MODEL

The Registry system supports a fine-grained permission model controlling access to each specific command. By default, clients receive access to all functionality; however it is possible to remove access to a specific command in response to abuse or threat to stability of the system. Clients that attempt a command they have lost permission to execute, receive an EPP command failed response indicating loss of authorisation.

8. COMPLIANCE

Compliance with EPP RFCs is achieved through design and quality assurance (QA).The EPP interface was designed to validate all incoming messages against the respective XML Schema syntax. The XML Schema is copied directly from the relevant RFCs to avoid any ambiguity on version used. Inbound messages that are either malformed XML or invalid are rejected with a 2400 response. Outbound messages are validated against the XML Schema, and if an invalid response is generated, it is replaced with a known valid pre-composed 2400 response, and logged for later debugging.
A QA process provides confidence that changes don't result in regressions in the interface. Automated build processes execute test suites that ensure every facet of the EPP service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs and the EPP service specification. These tests are executed prior to committing code and automatically nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging process.
New versions of the EPP Service follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars are encouraged during this stage to test their systems operate correctly. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior reaching production.
ARI surveys Registrars for information about the EPP client toolkit. These surveys indicated that while many Registrars use ARI toolkits, several Registrars use either their own or that from another registry. The ability for Registrars to integrate with the ARI EPP service without using the supplied toolkit indicates the service is compliant with RFCs.
ARI is committed to providing an EPP service that integrates with third party toolkits and as such tests are conducted using said toolkits. Any issues identified during testing fall into the following categories:

* Third-party toolkit not compliant with EPP
* EPP service not compliant with EPP
* Both third-party toolkit and EPP service are compliant, however another operational issue causes an issue

Defects are raised and change management processes are followed. Change requests may also be raised to promote integration of third-party toolkits and to meet common practice.

9. CAPACITY

.Hotel is projected to reach 26,715 domains at its peak volume and will generate 18.7 EPP TPS. This will consume 0.13% of the EPP resources of the SRS infrastructure. ARI's SRS can easily accommodate this. These numbers were described in considerable detail in the capacity section of Q24.

10 RESOURCES

This function will be performed by ARI. ARI provides a technical support team to support Registrars and also provides Registrars with a tool kit (in Java and C++) implementing the EPP protocol. Normal operations for all Registry Services are managed by ARI's Production Support Group (PSG), who ensure the EPP server is available and performing appropriately.

Faults relating to connections with or functionality of the EPP server are managed by PSG. ARI monitors EPP availability and functionality as part of its monitoring practices, and ensures PSG staff are available to receive fault reports from Registrars any time. PSG has the appropriate network, Unix and application (EPP and load balancing) knowledge to ensure the EPP service remains accessible and performs as required. these ARI departments support EPP:

* Products and Consulting Team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q25 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Hotel projects 26,715 domains, 0.05% of these resources are allocated to this TLD. See attachment 'Q25 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q25.

26. Whois

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background information on ARI please see the attachment 'Q26_ARI Background & Roles.pdf'. This response describes the Whois interface as implemented by ARI.

1. INTRODUCTION

ARI's Whois service is for all domain names, contacts, nameservers and Registrars provisioned in the Registry database. This response describes the port 43, web and searchable whois interfaces, security controls to mitigate abuse, compliance with bulk access requirements for registration data, and the architecture delivering the service.

2. PORT 43 WHOIS SERVICE

Whois is available on TCP port 43 in accordance with RFC3912. Requests are made in semi-free text format and terminated by an ASCII CR & LF. The server responds with a semi-free text format, terminating the response by closing the connection.
To support Internationalised Domain Names and Localised Registration Data we assume the query is encoded in UTF-8 and sends responses encoded in UTF-8. UTF-8 is backwards compatible with the ASCII charset and its use is consistent with the IETF policy on charsets as defined in BCP 18 [http://tools.ietf.org/html/bcp18].

2.1 Query Format

By default Whois searches for domains. To facilitate the queries of other objects a keyword must be included before the search string. Supported keywords are:
* Domain
* Host/Nameserver
* Contact
* Registrar
Keywords are case-insensitive. The remainder of the input is the search string. Wildcard chars may be used in search strings to match zero or more chars (%), or match exactly one char. Wildcard chars must not appear in the first 5 chars.

2.2. RESPONSE FORMAT

The response consists -
* An object-specific response represented by multiple key/value pairs. Where no object could be found the response is 'No Data Found'
* query-related meta-information to identify data freshness
* legal disclaimer
This format is consistent with that prescribed in the Registry agreement.

2.3, DOMAIN DATA

Domain data is returned in response to a query with the keyword omitted, or with the 'domain' keyword. Domain queries return information on domains that are provisioned in the Registry database.
The IDN domains may be specified in either the ASCII-compatible encoded form or the Unicode form. Clients are expected to perform any mappings, in conformance with relevant guidelines such as those specified in RFC5894 and UTS46.
Variant domains may be specified in the search string and Whois will match (using case-insensitive comparison) and return information for the primary registered domain.
For queries containing wildcard chars, If only one domain name is matched its details are returned, If more than one domain name is matched then the first 50 matched domain names are listed.

2.3.1. INTERNATIONALISED DOMAIN NAMES

The Whois response format, prescribed in Specification 4, does not provide a mechanism to identify active variant domain names. ARI will include active variant domain names in Whois responses until a common approach for handling and display of variant names is determined.

2.3.2. RESERVED DOMAIN NAMES

Domain names reserved from allocation will have a specific response that indicates the domain is not registered but also not available.

2.4. NAMESERVER DATA

Nameserver data is returned in response to a query where the 'nameserver' or 'host' keywords have been used. Nameserver queries return information on hosts that are provisioned in the Registry.
The search string for a nameserver query can be either a hostname or IP. Queries using the hostname produce one result unless wildcards are used. Queries using the IP produce one or more results depending on the number of hostnames that match that address. Queries for the hostname are matched case-insensitively.
The quad-dotted notation is expected for IPv4 and the RFC3513 – IPv6 Addressing Architecture format for IPv6. Wildcards cannot be used for IP queries.

2.5. CONTACT DATA

Contact data is returned in response to a query where the 'contact' keyword was used. Contact queries return information on contacts that are provisioned in the Registry.
The search string for a contact query is the contact identifier. Contact identifiers are matched using a case-insensitive comparison. Wildcards cannot be used.

2.6. REGISTRAR DATA

Registrar data is returned in response to a query where the 'Registrar' keyword was used. Registrar queries return information on Registrar objects that are provisioned in the Registry.
The search string for a Registrar query can be name or IANA id. Queries using the name or the IANA id produce only one result. Queries for the name are matched using a case-insensitive comparison. Wildcards cannot be used.

2.7. NON-STANDARD DATA

The SRS supports domain-related data beyond that above. It may include information used to claim eligibility to participate in the sunrise process, or other arbitrary data collected using the Key -Value Mapping to the EPP. This information will be included in the Whois response after the last object-specific data field and before the meta-information.

3. WEB-BASED WHOIS SERVICE

Whois is also available via port 80 using HTTP, known as Web-based Whois. This interface provides identical query capabilities to the port 43 interface via an HTML form.

4. SECURITY CONTROLS

Whois has an in-built mechanism to blacklist malicious users for a specified duration. Blacklisted users are blocked by source IP address and receive a specific blacklisted notification instead of the normal Whois response.
Users may be blacklisted if ARI's monitoring system determines excessive use. A whitelist is used to facilitate legitimate use by law enforcement agencies and other reputable entities.

5. BULK ACCESS

The Registry system complies with the requirements for the Periodic Access to Thin Registration Data and Exceptional Access to Thick Registration Data as described in Specification 4.

5.1. PERIODIC ACCESS TO THIN REGISTRATION DATA

ARI shall provide ICANN with Periodic Access to Thin Registration Data. The data will contain the elements as specified by ICANN. The format of the data will be consistent with the format specified for Data Escrow. The Escrow Format prescribes an XML document encoded in UTF-8. The generated data will be verified to ensure that it is well formed and valid.
The data will be generated every Monday for transactions committed up to and on Sunday unless otherwise directed by ICANN. The generated file will be made available to ICANN using SFTP. Credentials, encryption material, and other parameters will be negotiated between ARI and ICANN using an out-of-band mechanism.

5.2 Exceptional Access to Thick Registration Data

If requested by ICANN, ARI shall provide exceptional access to thick registration data for a specified Registrar. The date will contain full information for the following objects:

* Domain names sponsored by the Registrar
* Hosts sponsored by the Registrar
* Contacts sponsored by the Registrar
* Contacts linked from domain names sponsored by the Registrar

As above the format of the data will be consistent with the format specified for Data Escrow. And will be made available to ICANN using SFTP.

6. CAPACITY

ARI's Whois infrastructure is built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience running a high volume ccTLD registry (.au) and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [http:⁄⁄www.icann.org⁄en⁄resources⁄registries⁄reports we know there is:

* An average of 30 Whois txs per domain, per month.

Which indicates an expected monthly transaction volume of 600M txs For a registry with 20M DUMs

Through conservative comparison of .au registry numbers and the .net RFP response - specifically http:⁄⁄archive.icann.org⁄en⁄tlds⁄net-rfp⁄applications⁄sentan.htm we also know:

* The peak daily transactions is 6% of the monthly total (.au:6%, .net: 5%)
* The peak 5 min is 5% of the peak day (.au:5%, .net: 0.6%)

Thus we expect a peak WhoIs tx rate of 6,000 TPS.

For perspective on the conservativeness of this, the following numbers were taken from data in the May 2011 ICANN reports referenced above:

* .info ~7.8M domain names, peaks at ~1,300 TPS (projected peak TPS of ~3,400 with 20M names).
* .mobi ~1M domain names, peaks at ~150 TPS (projected peak TPS of ~3,000 TPS with 20M names).
* .org ~9.3M domain names, peaks at ~1,300 TPS (projected peak TPS of ~2,800 with 20M names).

After performing this analysis the projected TPS for .info was still the largest value seen. ARI's estimated value of 6,000 TPS for a registry with 20M Domains is roughly twice that of the .info projected peak of ~3400 TPS.

ARI benchmarked their WhoIs infrastructure and used the results to calculate the required computing resources for each of the tiers within the WhoIs architecture — allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server within the architecture, as well as the network bandwidth and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions and head room for growth. Despite doubling numbers, effective estimated capacity is still reported as 20 million domain names. The technical resource allocations are explored in question 32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.
.Hotel is projected to reach 26,715 domains at its peak volume and will generate 8 WhoIs transactions per second. This will consume 0.13% of the resources of the WhoIs infrastructure. As is evident ARI's WhoIs can easily accommodate this TLD's growth plans. See attachment 'Q26_Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's WhoIs infrastructure will be only 60% utilized. The WhoIs infrastructure capacity can also be easily scaled as described in question 32

7. ARCHITECTURE

Whois uses a separate replica database independent of the SRS database. Oracle Data Guard ensures the two databases are synchronised in real-time. The Whois service is operated live from the SRS 'failover' site, with the SRS 'primary' site serving as the 'failover' site for the Whois service. Both sites have enough capacity to run both services simultaneously. The architecture and data flow diagrams are described below and shown in the attachment 'Q26 – WhoIs.pdf'

Traffic enters the network from the Internet through border routers and then firewalls. All traffic destined for this service except for TCP ports 43, 80 & 443 is blocked. Load balancers forward the request to one of the application servers running ARI built Whois software. Each server is connected to the database cluster through another firewall further restricting access to the. Each server uses a restricted Oracle user that has read only access to the Registry data and can only access the data that is relevant to the Whois queries. This ensures that in the unlikely event of an application server compromise the effects are limited.

All components are configured and provisioned to provide N+1 redundancy. Multiple Internet providers with separate upstream bandwidth suppliers are used. At least one additional component of all hardware exists, enabling maintenance without downtime. This configuration provides a service exceeding the availability requirements in Specification 10.

The use of load balancing allows addition of application servers with no downtime. From a database perspective, the ability to scale is enabled by utilising Oracle RAC database clustering.
The entire service, including routers, firewalls and application layer is IPv6 compatible and Whois is offered on both IPv4 and IPv6 interfaces. Detail about this architecture is available in our response to Question 32.

7.1. SYNCHRONIZATION

The Whois database is synchronised with the SRS database using Oracle Data Guard. Committed transactions in the SRS database are reflected in the Whois database in real-time. Should synchronisation break, Whois continues to operate with the latest available data until the issue is reconciled. The channel between the two sites consists of two independent dedicated point to point links as well as the Internet. Replication traffic flows via the dedicated links or if both links fail replication traffic flows over Internet tunnels.

7.2. INTERCONNECTIVITY WITH OTHER SERVICES

The WhoIs service is not directly interconnected with other registry services or systems. The software has been developed to provide the WhoIs service exclusively and retrieve response information from a database physically separate to the SRS transactional database. This database is updated as described in 'Synchronisation' above. The WhoIs servers log every request to a shared central repository that is logically separate from the WhoIs database. This repository is used for query counts, detection of data mining and statistical analysis on query trends.

7.3. IT AND INFRASTRUCTURE RESOURCES

The WhoIs service is provided utilizing Cisco networking equipment, IBM application servers &, IBM database servers and SAN. They are described in the attachment 'Q26 - WhoIs.pdf'. For more information on the IT infrastructure including server specifications and database capabilities please see Q32 & Q33.

8. COMPLIANCE

Compliance with WhoIs RFCs is achieved through design and QA.
QA processes provide confidence that any changes to the service don't result in regression issues. Automated build processes execute test suites, prior to the committing of code and nightly, that ensure every facet of the WhoIs service is covered and compliant with RFCs. The final deliverable

is packaged and tested again.
New versions follow a deployment schedule. The new version is deployed into an OT&E environment for registrar integration testing. After a fixed time in OT&E without issue, they are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments.
ARI is committed to providing a WhoIs service that integrates with third party tools without issue and as such tests are conducted using third party tools such as jWhoIs, a popular UNIX command line WhoIs client.
Defects are raised and follow the change management process for all issues where the WhoIs service has been determined to not comply with the RFCs.

9. SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service restricted to pre-authorised clients.

9.1. DESCRIPTION OF SERVICE

The service provides search capabilities defined in Specification 4 and allows for:

* Exact-match on the registrar id, name server name, and name server's IP address;
* Partial-match on domain name, contacts, address (street, city, state or province, postcode, country); and
* Boolean search capabilities.

Matches for contact name and all postal address fields are case-insensitive. The client is restricted to one concurrent search to prevent unnecessary load on the system. The results include a list of domain names that match the criteria. The service allows for addition or removal of search criterion to meet local laws.

9.2. AUTHORISATION OF CLIENTS

Potential clients will request access to this service by providing the following on fax:
* Name
* Organisation
* Position
* Contact information
* Reason
* Query volume
* IP address

Access will be approved after background checks. Access is logged and monitored to protect against abuse. The use of HTTPS is enforced for the entire service.

Periodic audits of query logs will be used to identify any occurrences of data mining to suspend abusive clients.

10. RESOURCES

This function will be performed by the following ARI departments:
* Products and Consulting team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)
* Legal, Abuse and Compliance Team (6 staff)
and the following departments outsourced to the Directi Group:
* Abuse and Compliance Team (20 staff)

The products and consulting team is responsible for product management of the Whois solution including working with clients and the industry to identify new features or changes required to the system.

ARI employ a development team responsible for the maintenance and continual improvement of the Whois software

ARI's Production Support Team ensures the successful operation of the Whois system. The team comprises Database Administrators, Systems Administrators and Network Administrators. This team routinely checks and monitors bandwidth, disk and CPU usages to plan and respond to expected increases in the volume of queries, and perform maintenance of the system including security patches and failover and recovery testing.

The Directi Group and ARI Abuse and compliance teams provide abuse monitoring detection mechanisms to block data mining. Additionally the support team in conjunction with both the Compliance teams

administer requests for listing on the Whitelist, as well as requests for access to the searchable whois

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q26_ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Hotel projects 26,715 domains, 0.05% of these resources are allocated to this TLD. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

11. FINANCIAL COSTS
The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q26.

27. Registration Life Cycle

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background please see attachment 'Q27_ARI Background & Roles.pdf'. This response describes the Registration Lifecycle as implemented by ARI.

1. INTRODUCTION

The lifecycle described matches current gTLD registries. All states, grace periods and transitions are supported by the EPP protocol as described in RFC5730 - 5734 & the Grace Period Mapping published in RFC3915. An overview is in attachment 'Q27 – Registration Lifecycle.pdf'.

2. REGISTRATION PERIODS

The Registry supports registration up to 10 years and renewals for 1 to 10 years. Transfers extend registration by 1 year. The total validity period can't exceed 10 years.

3. STATES

The states that a domain can exist in are: Registered, Pending Transfer, Redemption, Pending Restore & Pending Delete.

All domain name statuses (RFC 3915, 5730-5734 and 5910) are covered below

3.1 REGISTERED

EPP Status: ok
In DNS: Yes
Allowed Operations: Update, Renew, Transfer (request) & Delete
The default state of a domain - No pending operations. The Sponsoring Registrar may update the domain.

3.2 PENDING TRANSFER

EPP Status: pendingTransfer

In DNS: Yes
Allowed Operations: Transfer (cancel, reject, approve)
another Registrar has requested transfer of the domain and it is not yet completed all transform operations, other than those to cancel, reject, or approve the transfer are rejected.

3.3 REDEMPTION

EPP Status:pendingDelete
RGP Status:redemptionPeriod
In DNS:No
Allowed Operations:Restore (request)

Domain has been deleted. The sponsor may request restoration of the domain. The domain continues to be withheld from the DNS unless restored. No transform operations other than restore allowed.

3.4 PENDING RESTORE

EPP Status:pendingDelete
RGP Status:pendingRestore
In DNS:No
Allowed Operations:Restore (report)
a restore request is pending. Sponsor must submit a restore report. The domain remains withheld from the DNS. No transform operations other than restore report allowed.

3.5 PENDING DELETE

EPP Status:pendingDelete
RGP Status:pendingDelete
In DNS:No
Allowed Operations:None
the Redemption Grace Period has lapsed and the domain is pending purge from the Registry. This state prohibits the sponsor from updating, restoring or modifying the domain for 5 days. At the end of this period the domain is purged and made available for registration.

4. GRACE PERIODS

The Registry system supports 4 grace periods: add, renew, auto-renew, and transfer, described below with consideration for overlap of grace periods. States described here are additional to those above.

4.1 ADD GRACE PERIOD

Length:5 days
RGP Status:addPeriod
Allows for the no-cost cancellation of a domain to rectify errors within 5 days from registration. The following rules apply for operations during this period:

* Delete: Sponsoring Registrar may delete the domain with immediate effect and receive a refund subject to the Add Grace Period Limits consensus policy.
* Renew: sponsor may renew the domain and is charged for the operation. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy.
* Bulk Transfers: A bulk transfer is permitted during the Add Grace Period as per ICANN policy, and causes the Add Grace Period to not apply.

4.2 RENEW GRACE PERIOD

Length:5 days
RGP Status:renewPeriod
Allows the Sponsoring Registrar to undo a renewal within 5 days of the renewal command. The following rules apply for operations during this period:

* Delete: Sponsoring Registrar may delete the domain and receive a refund. The extension caused by the preceding renew is reversed and unless the domain is also in the Add Grace Period, the domain enters the Redemption state. If in the Add Grace Period it is deleted with immediate effect and available for registration.
* Renew: sponsor can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: an approved transfer command ends the current Renew Grace Period without a refund and

begins a Transfer Grace Period.
* Bulk Transfers: cause the Renew Grace Period to end without a refund, consequently registration periods are not changed.

4.3 AUTO-RENEW GRACE PERIOD

Length:45 days
RGP Status:autoRenewPeriod
Allows for domains to remain in the DNS past expiration giving time for the Registrar to obtain renewal confirmation from the Registrant.
This period lasts for 45 days after expiration. The following rules apply for operations during this period:

* Delete: the Registrar, may delete the domain and receive a refund. The domain enters the Redemption state.
* Renew: the Registrar can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: an approved transfer command ends the current Auto-Renew Grace Period with a refund to the losing Registrar and begins a Transfer Grace Period. The registration period auto-renew extension is reversed and the registration is extended by the period specified in the transfer.
* Bulk Transfers: bulk transfers cause the Auto-Renew Grace Period to end without a refund consequently registration periods are not changed.

4.4 TRANSFER GRACE PERIOD

Length: 5 days
RGP Status:transferPeriod
Transfer Grace Period allows the Sponsoring Registrar to undo the registration period extension (due to a transfer command), via the deletion of a domain within 5 calendar days. The following rules apply for operations during this period:

* Delete: the Registrar may delete the domain and receive a transfer fee refund. The extension to the registration period of the preceding transfer is reversed and the Redemption state is entered.
* Renew: the Registrar can renew the domain causing a Renewal Grace Period to begin. The Registrar is charged and the total period is extended by the renewal term, limited to 10 yr maximum
* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy. Special situations requiring a transfer back to the losing Registrar are dealt with case by case manually.
* Bulk Transfers: bulk transfers cause the Transfer Grace Period to end without a refund; consequently registration periods are not changed.
The Transfer Grace Period does not have any impact on other commands.

4.5 REDEMPTION GRACE PERIOD

Length:30 days
RGP Status: as described in Redemption state
Redemption Grace Period refers to the period of time the domain spends in the Redemption state, starting after a domain is deleted. The Redemption state description provides information on operations during this period.

4.6 OVERLAP OF GRACE PERIODS

The 4 possible overlapping grace periods are:
* Add Grace Period with 1 or more Renew Grace Periods.
* Renew Grace Period with 1 or more other Renew Grace Periods.
* Transfer Grace Period with 1 or more Renew Grace Periods.
* Auto-Renew Grace Period with 1 or more Renew Grace Periods.
These are treated independently with respect to timelines however action that is taken has the combined effects of all grace periods still current.

4.6.1 TRANSFER CLARIFICATION

If several billable operations, including a transfer, are performed on a domain and it is deleted in the operations' grace periods, only those operations performed after/including the latest transfer are eligible for refund.

5. TRANSITIONS

5.1. AVAILABLE 〉 REGISTERED

Triggered by the receipt of a create command to register the domain. The Sponsoring Registrar is charged for the creation amount. this transition begins the Add Grace Period.

5.2 REGISTERED 〉 PENDING TRANSFER

Triggered by the receipt of a request transfer command. The transfer must result in domain registration extension — the gaining Registrar is charged for the transfer. Requests to transfer the domain within 60 days of creation or a previous transfer are rejected.

5.3 PENDING TRANSFER 〉 REGISTERED

Triggered by 1 of 4 operations:

* Cancel: the Gaining Registrar may cancel a transfer
* Reject: the Losing Registrar may reject the transfer
* Approve: the Losing Registrar may approve the transfer.
* Auto-Approve: If after 5 days, no action has been taken, the system approves the transfer.

In case of Cancel⁄Reject. The Gaining Registrar is refunded the transfer fee. The registration period remains unchanged and all grace periods existing at the time of transfer request remain in effect if not elapsed.

In case of Approve ⁄ Auto-Approve if the transfer was requested during the Auto-Renew Grace Period, the extension to the registration period is reversed and the Losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified. This begins the Transfer Grace Period.

5.4 REGISTERED 〉 DELETED

On receipt of a delete command if the domain is in the Add Grace Period, it is purged from the Database and immediately available for registration.

5.5 REGISTERED 〉 REDEMPTION

On receipt of a delete command if the domain is not in the Add Grace Period, it transitions to the Redemption Period state and all grace periods in effect are considered.

5.6 REDEMPTION 〉 PENDING RESTORE

On receipt of a restore command if the Redemption Period has not lapsed, the domain transitions to the Pending Restore state. The Sponsoring Registrar is charged a fee for the restore request.

5.7 PENDING RESTORE 〉 REGISTERED

During the Pending Restore period the Sponsoring Registrar may complete the restore via a restore report containing the Whois information — submitted prior to the deletion, the Whois information at the time of the report, and the reason for the restoration.

5.8 PENDING RESTORE 〉 REDEMPTION

Seven calendar days after the transition to the Pending Restore state, if no restore report is received the domain transitions to the Redemption state, which begins a new redemption period. The restore has no refund.

5.9 Redemption 〉 Pending Delete

Thirty calendar days after the transition to the Redemption state, if no restore request is received the domain transitions to the Pending Delete state.

5.10 PENDING DELETE 〉 DELETED

Five calendar days after the transition to the Pending Delete state, the domain is removed from the Database and is immediately available for registration.

6. LOCKS

Locks may be applied to the domain to prevent specific operations. The Sponsoring Registrar may set the locks prefixed with ‘client’ while locks prefixed with ‘server’ are added and removed by the Registry Operator. Locks are added and removed independently but they can be combined to facilitate the enforcement of higher processes, such as ‘Registrar Lock’, and outcomes required as part of UDRP. All locks are compatible with EPP RFCs. The available locks are:

* clientDeleteProhibited, serverDeleteProhibited - Requests to delete the object are rejected: -
clientHold, serverHold - : DNS information is not published
* clientRenewProhibited, serverRenewProhibited - : Requests to renew the object are rejected. Auto
-renew is allowed
* clientTransferProhibited, serverTransferProhibited - : Requests to transfer the object are
rejected
* clientUpdateProhibited, serverUpdateProhibited - : Requests to update the object are rejected,
unless the update removes this status

7. TYPICAL REGISTRATION LIFECYCLE

A typical domain is provisioned immediately on registration. The domain name may be updated over its lifetime to reflect changes in contact or delegation information. The domain name will remain active in the registry by automatic renewals once the registration period has lapsed however Registrars may elect to explicitly renew the domain before the automatic renewal or to extend the registration period by more than one year. The registrar may delete the domain following non-payment or request from the registrant resulting in the immediate removal from the DNS. A time-delayed set of server events will result in the purging of the name from the registry database if the name is not restored during a 30-day redemption period.

8. SPECIAL CONSIDERATIONS

8.1 ICANN-APPROVED BULK TRANSFERS

ICANN-Approved Bulk Transfers performed in accordance with Part B of the Inter-Registrar Transfer Policy do not follow the typical transfer lifecycle. Existing grace periods are invalidated and no refunds are credited to the Losing Registrar. The prohibition of transfer period on domains created or transferred within 60 days does not apply.

8.2 UNIFORM RAPID SUSPENSION

In the Uniform Rapid Suspension (URS) process, as described in the ‘gTLD Applicant Guidebook’ the following modification to the above processes is required.
Remedy allows for the addition of a year to the registration period, limited to the 10 year maximum. During this time no transform operations may be performed other than to restore the domain as allowed by Appeal. At the expiration of the registration period the domain is not automatically renewed, but proceeds to the Redemption state as per the lifecycle described above, and it is not eligible for restoration.

9. UPDATE⁄DNS

The update command does not impact the state of the domain through the Registration Lifecycle, however the command can be used to add and remove delegation information, which changes the DNS state of the domain.

10. RESOURCES

This function will be performed by the following ARI departments:
* Products and Consulting team (7 staff)
* Development Team (11 staff)
the following departments outsourced to the Directi Group:
* Abuse and Compliance Team (20 staff)

ARI’s Registry performs all time-based transitions automatically and enforces all other business rules — without requiring human resources for normal operation. If changes to the automatic behaviours or restrictions enforced by the policy system are required, ARI has a development team for this.

Domain Name Lifecycle aspects requiring human resources to manage are included in the ARI outsourcing include:
* Processing Add Grace Period exemptions as requested by Registrars.
* Processing restore reports provided by Registrars.
* Meeting the Registry Operators obligations under ICANN’s Transfer Dispute Policy.
* Performing exception processing in the case of approved transfers during the 60 day transfer prohibition window.

The Products and Consulting team is responsible for product management of the Registration Lifecycle, including working with clients and the industry to identify new features or changes required to the system.

The automated aspects of the Registration lifecycle are supported by ARI's Domain Name Registry software. ARI has a development team for maintenance and improvement of the software

Most manual tasks fall to the Abuse and Compliance teams of the Directi Group, with staff experienced in development of policy for policy rich TLD environments. They have the required legal and industry background to perform this function.

The Compliance team outsourced to the Directi Group is responsible for any abuse of the registration policies within .Hotel and supervising the role of any external agency involved in validation

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q27_ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Hotel projects 26,715 domains, 0.05% of these resources are allocated to this TLD. See attachment 'Q27 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q27.

28. Abuse Prevention and Mitigation

DotHotel Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. The Directi Group manages centralized functions for all its businesses. We have outsourced our Abuse and Compliance functions to the Directi Group and our Abuse and Compliance desk will be staffed as a cost center by them.

This response aims to provide a 360 degree perspective on our policies and processes to prevent abusive activities, and ensure swift mitigation when abuse does occur. We have prepared this plan based on over a decade's experience of fighting abuse as a Registrar, learnings through active industry participation, best-practices from existing registry operators and expert inputs from our back-end technical partner ARI (AusRegistry International).

1. ABUSE MITIGATION EXPERIENCE AND CAPABILITIES

With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain names and is fully cognizant of the threat that stems from their abuse.
As one of the world's top ten registrars, we equally understand our ability to make a sizable contribution towards curbing internet abuse, and believe that mitigating this threat is one of our foremost responsibilities. By instituting policies, processes and services which go significantly above and beyond our obligation as a registrar, Directi has taken various initiatives to make the Internet a safer ground.
To drive this effort, Directi has a committed function working towards identifying abusive domain names and enforcing its policies. Our Abuse Desk functions 24⁄7 and takes prompt and effective

action (both reactively and proactively) against domains reported or co-networked to be involved in any sort of online abuse. Complaints ranging from phishing, spam, malware perpetration, 419 scams, child pornography, copyright infringement and varied forms of abuse are subject to investigation at our Abuse Desk on a daily basis. The nature of abuse and the types of complaints received are varied in nature and intensity, and are documented in more detail further.
On average we already address, 15000 reported or detected abuse cases per year. Abuse cases are addressed within pre-determined SLAs, and our team is committed to ensure that each incident is resolved satisfactorily. The Directi abuse team has been heralded on many occasions by various security groups, law enforcement organizations and the general anti-abuse community for the manner in which abuse mitigation has been handled by us. Additionally, we have always become highly involved, and continue to remain committed to industry-wide efforts to address organized abuse such as botnets (see below) and large scale phishing attacks, and any other malfeasances.

1.1 NOTABLE INSTANCES OF DIRECTI'S SUCCESSFUL ABUSE MITIGATION INITIATIVES

Our abuse mitigation team has developed strong relationships with many security groups and individuals in the abuse mitigation community, with the aim of sharing intelligence and facilitating quick action on abusive domain names. These sources provide us actionable intelligence on domains bought through our registrar. We have also participated in coordinated takedowns with such agencies in the past and are committed to doing so in the future. Please refer to Attachment 'Q28_Recommendations' which showcases letters from several global agencies including the IRS, commending our work and cooperation on several fronts. Following are some examples of cases where our efforts paid great results in abuse mitigation –

1.1.1 MARIPOSA WORKING GROUP

Directi was part of the Mariposa Working Group which was responsible for taking down the largest known botnet network at the time.
(Ref: http://defintel.com/docs/Mariposa_White_Paper.pdf)

"Directi is BY FAR THE BEST registrar we have ever worked with at taking down criminal domains in a timely, efficient and professional manner. Your team was absolutely key to the Mariposa Working Group taking down one of the largest Botnets in the history of the Internet. You and your team should be VERY proud of that :)" -- ChristopherDavis, Former CEO of Defence Intelligence

1.1.2 IM WORM BOTNET TAKEDOWN COORDINATED BY IID

Since 1996, IID (Internet Identity) has been providing technology and services that secure the Internet presence for an organization and its extended enterprise. It recently introduced a number of unique approaches to secure organizations' use of Internet infrastructure with ActiveTrust® BGP, ActiveTrust DNS, and ActiveTrust Resolver with TrapTrace. Directi worked with IID, acting against problematic domain names and sharing intelligence to take down a notorious botnet that was plaguing the internet for quite some time.

"Thank you for your exceptional coordination with our team and the other providers … during the simultaneous shutdown. We wanted to follow up with you and let you know that despite the last minute unanticipated scramble, the takedown was a success and the botnet has been shutdown." -- Lauren Lamp, Manager / Service Delivery -internetidentity.com

1.1.3 FAKE PHARMACY TAKEDOWNS COORDINATED BY LEGITSCRIPT

LegitScript is the leading source of information for patients, Internet users, physicians, businesses and other third parties who need to know if an Internet pharmacy is acting in accordance with the law and accepted standards of ethics and safety. LegitScript is identified by the National Association of Boards of Pharmacy as the only Internet pharmacy verification service that adheres to its standards. After affiliating with LegitScript, we have witnessed a steep downfall in fake pharma-related registrations. ResellerClub (referred below) is our wholesale registrar brand.
(Ref:http://legitscriptblog.com/2009/03/directi-no-safe-haven-for-rogue-internet-pharmacies/)

"Some registrars claim that they cannot shut down dangerous 'no-prescription-required' and fake online pharmacies. ResellerClub has proven that this is not true. By refusing to profit from dangerous, criminal activity at the expense of Internet users, ResellerClub has established itself as a responsible example for the rest of the
Internet community." John Horton, President, LegitScript.com

We have enclosed a commendation letter from LegitScript in Attachment 'Q28_Recommendations', which speaks of our leadership in fighting fake and rouge pharmacies.

1.1.4 419 FEEDBACK LOOP WITH ARTISTS AGAINST 419 (AA419.ORG)

An honorary member of the APWG (Anti-Phishing Working Group), Artists Against 419 is a premier organization with expertise in identifying, cataloging, and terminating fraud sites. Our tie-up with them has been greatly successful in eliminating fraudulent registrations within our portfolio. (Ref: http://blog.aa419.org/?p=134)

"Many registrars do respond to abuse reports and take action against them. However none do it as quickly and efficiently as Directi. If all registrars and hosters take this approach, it might then be possible to reduce internet fraud." -- aa419.org

We have enclosed a letter from Artists Against 419 in Attachment 'Q28_Recommendations', commending the speed and impact of our proactive abuse mitigation activities.

2. PROPOSED ABUSE POLICY FOR .HOTEL

We have fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010).

Our abuse policies described in this section apply to initial and ongoing domain registrations, i.e. any domain name must comply with these policies during registration and throughout its tenure.

Abusive behaviour in a TLD may relate can be categorized into:

2.1. REGISTRATION POLICY VIOLATIONS

.Hotel adopts certain Registration policies and any violations of these policies would be treated as an Abuse.

2.1.1. SUNRISE POLICY VIOLATION

.Hotel will have a sunrise period as described in the response to Question 29. Our sunrise policy will have an overarching goal to protect interests of IP holders globally, and be based on best practices seen in previous TLD launches. We will implement the Trademark Claim Service and partner with experienced service providers to run the TM verification, Sunrise Challenge and Auction processes. All Sunrise domain names will be validated before they are activated. Hence the possibility of a Sunrise policy violation is low. However the Sunrise process provides for a Sunrise Dispute Resolution Policy, and any disputes that fall within its scope will be referred to the Sunrise Dispute Resolution provider. If the abuse desk receives any complaints concerning a sunrise domain which violates the Sunrise eligibility policy the abuse desk will direct the complainant to the Sunrise Dispute Resolution provider

2.1.2. WHOIS INACCURACY

.Hotel requires Whois accuracy as per its contracts. Any domain name with inaccurate whois information will be deemed to be in violation of its contract and hence will be deemed as an abuse and handled in the manner described ahead.

2.1.3. TRADEMARK INFRINGEMENT VIOLATION AND UDRP

.Hotel requires registrants to abide by UDRP. If the abuse desk receives any complaints concerning a domain name which infringes upon the trademark right of a 3rd party, the abuse desk will direct the complainant to the Uniform Dispute Resolution provider.

All names registered under .Hotel will be subject to the UDRP and URS processes. We believe that URS will deter cybersquatting, and some malicious activities that illegitimately use brand names. We will seek to expeditiously process all URS cases, and are already equipped with mature processes and tracking systems to manage and keep track of all cases.

The URS process will be run by our compliance team, who has significant experience in processing UDRP complaints for our Registrar businesses.

While Registrars will be responsible for processing all UDRP cases related to .Hotel, we will reserve the right to act on their behalf when necessary, and process all court orders that are directed to us.

2.1.4 ELIGIBILITY RESTRICTIONS

The eligibility criteria for registering general names within .hotel is defined in our response to

Q29. Any general domain name Registrant that does not fulfill the defined criteria is considered as abuse.

If the abuse desk receives any complaints concerning a domain name which violates the Eligibility Restrictions Policy the abuse desk will direct the complainant to a Eligibility and Restrictions Dispute Resolution Provider appointed by us.

2.2. ACCEPTABLE USAGE RELATED VIOLATIONS

.Hotel adopts certain Content and Acceptable usage policies and any violations of these would be treated as an Abuse. The following are deemed as violations of our content and acceptable usage policy

2.2.1. Intellectual property, Trademark, Copyright, and Patent violations, including piracy

Intellectual property (IP) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation or any other harmful act by any individual or a company is categorized as Intellectual Property violation.

2.2.2. SPAMMING

The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and⁄or charitable requests and requests for assistance are also considered as spam.

2.2.3. PHISHING (and various forms of identity theft)

Fraudulent web services and applications meant to represent⁄confuse or mislead internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

2.2.4. PHARMING AND DNS HIJACKING

Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

2.2.5. DISTRIBUTION OF VIRUSES OR MALWARE

Most typically the result of a security compromised web service where the perpetrator has installed a virus or “malevolent” piece of software meant to infect computers attempting to use the web service in turn. Infected computers are then security compromised for various nefarious purposes such as gaining stored security credentials or personal identity information such as credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services (see botnet below).

2.2.6. CHILD PORNOGRAPHY

Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

2.2.7. USING FAST FLUX TECHNIQUES

A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

2.2.8. RUNNING BOTNET COMMAND AND CONTROL OPERATIONS

A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm - ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command

and control refers to a smaller number of computers that issue/distribute subsequent commands to the Botnet. Compromised botnet computers will periodically check in with a command and control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.
Registries play a key role in breaking this cycle of pre-determined domain registrations by deactivating said registrations prior to the compromised computers being able to use them to contact the command and control computer. Successful intervention results in the botnet losing contact with their command and control computers, leaving them inactive and reducing potential harms.

2.2.9. HACKING

Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other individuals. Also includes any activity that might be used as a precursor to an attempted system penetration.

2.2.10. FINANCIAL AND OTHER CONFIDENCE SCAMS

Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are –
1. Ponzi Schemes. A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."
2. Money Laundering. Money laundering, the metaphorical "cleaning of money" with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy.
3. 419 Scams. "419" scam (aka "Nigeria scam" or "West African" scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as "Advance Fee Fraud". The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money that they would receive later if they cooperate.

2.2.11. ILLEGAL PHARMACEUTICAL DISTRIBUTION

Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution are termed illegal.

2.2.12. OTHER VIOLATIONS

Other violations that will be expressly prohibited under the .Hotel TLD include
* Network attacks
* Violation of applicable laws, government rules and other usage policies

3. PROCEDURES TO MINIMIZE ABUSIVE REGISTRATIONS

3.1. BUILDING A ZERO-TOLERANCE REPUTATION

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

Directi has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Hotel. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in violation of our policies are suspended rapidly, both abusive registrations and abusive behavior will be discouraged.

Our Abuse policies described in section 2 above apply to new and ongoing registrations.

3.2. BUILDING AWARENESS OF OUR ANTI-ABUSE POLICY

The Abuse Policy will be published on the abuse page of our Registry website which will be accessible and have clear links from the home page. The abuse page of our Registry website will

emphasise and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that the clear message, which communicates our commitment to combating abusive registrations, will further serve to minimize abusive registrations in our TLD.

3.3. ICANN PRESCRIBED MEASURES

In accordance with our obligations as a Registry Operator we will comply with all requirements in the 'gTLD Applicant Guidebook'. In particular, we will comply with the following measures prescribed by ICANN which serve to mitigate the potential for abuse in the TLD:

* DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy to use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43;
* Prohibition on Wild Carding as required by section 2.2 of specification 6 of the Registry Agreement

* Removal of Orphan Glue records: ICANN requires a policy and procedure to take action to remove orphan glue records from the zone when provided with evidence that the glue is indeed present and aiding malicious conduct. The ARI Managed TLD Registry SRS database does not allow orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the Registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid name server. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner

3.4. REGISTRANT DISQUALIFICATION

Abusive domain registration has historically attracted a small number of individuals and organisations that engage in high volume registrations, driven by the marginal profitability of individual abusive registrations. As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a Registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a Registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy.

Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations through the possible loss of all registrations.

In addition, name servers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

3.5. PROACTIVE DETERMINATION OF POTENTIAL ABUSE

There are several tell-tale signs which are indicative of abusive intent. The following are examples of the data variables will serve as indicators that we will monitor with the help of our registry technical partner.

* Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may when considered as a whole be indicative of abuse

* Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): Our service provider ARI uses the formula developed by the University of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.

* An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the

location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.

* Results of Monthly Checks: The random monthly checks to promote Whois accuracy (described ahead) are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate Whois data and abuse.

* Analysis of Cross Validation of Registrant Whois data against Whois Data Known to be Fraudulent.

* Analysis of Domain Names belonging to Registrant subject to action under the Anti-Abuse policy: in cases where action is taken against a registrant through the application of our Anti-Abuse policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

4. PROCEDURES FOR HANDLING COMPLAINTS

4.1 MECHANISMS FOR REPORTING COMPLAINTS

In order to make it easy for security agencies, law enforcement bodies and vigilant users to report incidents of abusive behavior within .Hotel, we shall enable several channels of communication.

4.1.1 SINGLE POINT OF CONTACT

In accordance with section 4.1 of specification 6 of the Registry Agreement we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, registrars, LEA (Law Enforcement Agencies), government and quasi governmental agencies and recognised members of the anti-abuse community.

The SAPOC's accurate contact details (email, fax and mailing address) will be provided to ICANN and published on the abuse page of our Registry website. The SAPOC will in turn represent the entire compliance desk operated by the Directi group on behalf of .Hotel as an outsourced function.

The Registry website will additionally also include:
* All public facing policies in relation to the TLD including the Anti-Abuse Policy described in section 2
* A web based submission service for reporting inaccuracies in Whois information
* Registrant Best Practices
* Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions

As such, the SAPOC may receive complaints regarding a range of matters concerning the abuse policy defined in section 2

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organization and the type of abuse. Accordingly, separate processes for identifying abuse will exist for reports by LEA⁄government and quasi governmental agencies and members of the general public.

When any party makes a report via the Abuse POC e-mail address or the abuse web form, he or she will receive back a ticket number from a ticketing system. Our abuse team will then examine these reports, and use a ticketing system to track each issue. This process will leverage a dedicated software that we have used for handling abuse reports to our registrar businesses. It is our goal to provide a timely response to all abuse complaints concerning domains registered in the TLD, as per the SLAs defined by us.

4.1.2 LAW ENFORCEMENT AGENCIES

We recognise that LEA, governmental and quasi governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for law enforcement, government and quasi-governmental agencies to, amongst other things, report

illegal conduct in connection with the use of the TLD.

The process will involve prioritization and prompt investigation of reports identifying abuse from those organizations. The steps in the expedited process are summarised as follows:

1. We will identify relevant LEA, government and quasi governmental agencies who may take part in the expedited process
2. We will establish back channel communication with each of the identified agencies in order to obtain information that may be used to verify the identity of the agency upon receipt of a report utilising the expedited process;
3. We will publish contact details on the abuse page of the Registry website for the SAPOC to be utilised by only those taking part in the expedited process;
4. All calls to this number will be responded to by a member of our 24⁄7 Compliance Team
5. We will verify the identity of the reporting agency employing methods specific to that agency established during back channel communication;
6. Upon verification of the reporting agency, we will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD;
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing
8. The report identifying abuse will then be dealt with in accordance to our process defined in subsequent sections of this answer

4.2. EVALUATION OF COMPLAINTS

The next step is for our abuse desk staff to review each complaint. The abuse team looks at the facts of each complaint in order to verify the complaint. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants while at the same time, taking timely action to mitigate abusive behaviour and to minimize impact.

Evaluation of complaints thus forms a very important part of the process. The following factors are considered for each case:
* Type, Severity and immediacy of the abuse: Upon initial review, all incoming complaints will face an initial evaluation on the basis of severity and harm cased due to the abuse. While we will adhere to the SLAs laid down for our abuse mitigation processes, regardless of the type of complaint, there will be some complaints that will be considered relatively more severe and of greater malicious impact than others. Complaints with a higher severity⁄malicious impact and immediacy will be processed with greater urgency than others.

* Determining the origin of the complaint: a credible complainant e.g. a law enforcement agency, a security group etc. automatically lends genuineness to a complaint while a complaint from a previously unknown source will require a background check to ensure that the complaint is not from a miscreant looking to create unnecessary trouble for a domain owner. Thus while we may take immediate action complaints from reliable sources, those from other sources, not backed by enough evidence, may require further due-diligence before action is taken.

* Evaluating proof submitted along with a complaint: A complaint is also evaluated based on the supporting evidence provided which further determines the validity of a complaint. At this stage we will also attempt to establish a clear link between the activity reported and the alleged type of abusive behaviour. This is done to ensure that addressing the reported activity will address the abusive behaviour. In some cases the abuse is evident, which will result in immediate processing of the complaint from our side without much further due-diligence. In some cases, where the abuse may not be evident upfront, our desk will rely on supplementary evidence provided by the complainant which may be further ratified. While not limited to this list, supporting evidence could range from links, screen-shots of websites, copy right ⁄ trademark details, emails, email headers, whois information, ID proof etc.

* Evaluating historical data: As mentioned before, we will maintain a log of all complaints received, including the contact details of complainants, the whois details of the abusers, the nameservers of abusive domain registrations, the type of domain names, the IPs of spamming domains etc. This will further help us in establishing trends for further action as required. A registration that re-sounds alarms from previously seen abusive trends will ascertain the necessary pre-emptive mitigation processes.

Assessing abuse reports requires good judgment, and we will rely upon our, specially trained abuse desk staff.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and

immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken accordingly. It must be emphasised that the actions to mitigate the identified type of abuse in the section⁄s below are merely intended to provide a rough guideline and may vary upon further investigation.

4.3. CATEGORIZATION OF COMPLAINTS

Each confirmed case of abuse is bucketed into one of the following categories

4.3.1. CATEGORY 1

Probable Severity or Immediacy of Harm - Low
Examples of types of abusive behaviour –Small Scale Spam, Whois Inaccuracy

Mitigation steps -
1. Preliminary Investigation
2. Delegate to Registrar
3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

4.3.2. CATEGORY 2

Probable Severity or Immediacy of Harm - Medium
Examples of types of abusive behaviour – Medium scale spam, inactive botnets and other forms of abuse which have a higher degree of impact than the ones bucketed as category 1, but still relatively limited in terms of potential damage.

Mitigation steps -
1. Preliminary Investigation
2. Delegate to Registrar
3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

4.3.3. CATEGORY 3

Probable Severity or Immediacy of Harm - High
Examples of types of abusive behaviour – Fast Flux Hosting, Phishing, Large scale hacking, Pharming, Botnet command and control, Child Pornography and all other cases deemed to carry a very high risk of large scale impact

Mitigation steps for Abuse policy violation -
1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

4.4. MITIGATION OF COMPLAINTS

The mitigation steps for each category will now be described:

4.4.1. CATEGORY 1

Types of abusive behaviour that fall into this category include those that represent a low severity or immediacy of harm to registrants and internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. Each of these cases will be delegated down to the Registrar and the registrar’s performance, in terms of response and resolution rate, will be monitored and recorded by us. In case of non-conformance by the Registrar, we will take-over the issue.

We will also continually monitor the issue to track possible increases in the severity of harm. In case the threat level is above what was originally anticipated, we will escalate the issue to category two or three and act in accordance.

4.4.2. CATEGORY 2

Types of abusive behaviour that fall into this category include those that represent a medium severity or immediacy of harm to registrants and internet users. These generally include medium scale spam, network intrusion, inactive botnets etc. Following the notification of the existence of such behaviours, our compliance team will delegate the issue to registrars and invoke the more aggressive SLAs that apply to this category of risk.

As was the case with category 1, we will continue to monitor the registrar's conformance with the SLAs and take direct action when necessary. We will also check for possible increases in risk levels and escalate the abuse category if required.

4.4.3. CATEGORY 3

Highly serious, sensitive and large scale issues like phishing, child pornography and large-scale botnet are considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities, high level of risk and far-reaching consequences. Given the direct relationship between the uptime of these activities, and extent of harm caused, we recognise the urgency required to execute processes that handle these cases directly, without any delegation.
As soon as the abuse is substantiated, we will proceed to suspend the domain name pending further investigation to determine whether the domain name should be unsuspended or cancelled.
Cancellation will result if upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti Abuse Policy.

In some cases we may change the nameservers associated with the domain and⁄or use EPP prohibited statuses in appropriate combinations to restrict activity against the domain such as contact updates, deletes or transfers.

In the past we have modified Nameservers to sinkhole malicious domains, so research partners can measure botnets and monitor malware activity. We believe this to be an extremely effective mechanism which takes down large scale attacks from the source, and assists researchers to build processes and tools which prevent future attacks from the same source. Our team will follow the same process for domains belonging to our registry.

We have built special systems to suspend individual and bulk batches of domains. This will allow us to quickly take care of cases where criminals have obtained bulk batches of domain names. This will be of use if malware designers use generation algorithms to register domains.

Reactivation of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti Abuse Policy, does not exist and that the domain name is not causing any harm.

4.5. PROPOSED RESOLUTION METRICS AND SERVICE LEVEL AGREEMENTS

SLA RESPONSE CONSIDERATIONS FOR REPORTED ABUSE CASES
As described earlier, each abuse case and goes into one of three response categories depending on the severity and immediacy of the harm caused by the abuse. In the case of any failed SLA responses, the Registry reserves the right to act directly to suspend and⁄or lock the domains associated with a given abuse case. Additionally, highly serious, sensitive and large scale issues are ranked as category 3 and prioritized above all other cases.

Attachment'Q28_Abuse Mitigation SLA' shows the flowchart and SLA response for each category of abuse complaint

4.5.1. CATEGORY 1

Some examples of abuses cases that will be categorized as 1 include:

* Low scale Spam
* Whois Inaccuracy
* Low scale Malware
* Any other abuse case deemed as low risk

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
* Initial Response from Registrar: 3 business days from the time that the complaint notification is sent to the Registrar
* Update from Registrar as action taken or intended: 7 business days from the time that the complaint notification is sent to the Registrar
* Final Resolution: 15 business days from the time the issue was reported to us

4.5.2. CATEGORY 2

Some examples of abuses cases that will be categorized as 2 include:

* Medium scale Spam
* Confirmed but inactive botnet domains
* All other abuse cases deemed as medium scale

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
* Initial Response from Registrar: 2 business days from the time that the complaint notification is sent to the Registrar by the Registry
* Update from Registrar as action taken or intended: 3 business days from the time that the complaint notification is sent to the Registrar by the Registry
* Final Resolution: 8 business days from the time of receipt of the complaint

4.5.3. CATEGORY 3

Some examples of abuses cases that will be categorized as 3 include:

* Confirmed Cases of child pornography
* Confirmed cases of Phishing
* Confirmed and active botnets domains
* Any other case deemed as large scale

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 1 business day from the time of receipt of the complaint
* Registry time to direct takedown: 3 business days from the time of receipt of the complaint

4.6. Follow-up and Capture of Metrics

The abuse staff will track each abuse complaint ticket to resolution. Our ticketing system allows us to capture many metrics. We will measure resolution times, and we can see what percentage of abuse reports could be confirmed. We will also capture how many domains were suspended, and we will break down statistics by registrar in the TLD. This will help us identify registrars that have regular problems, and we can work with them to systematically identify and act against bad actors.

4.7. CONTRACTUAL PROVISIONS

As the registry operator, we will use the Registry-Registrar Agreement (RRA) to establish the registry's right to act against abusive registrations as described in the preceding sections. We will also use the contract to impose certain obligations on the registrars, and make some obligations binding on the registrants by obligating specific terms in the registrar-registrant contract. The contract will be a mandatory part of the Registrar accreditation process with the Registry. Production access to the Registry will not be granted until the contract is duly signed AND the registrar has provided copy of their Registry Registrant Agreement to demonstrate the inclusion of any required pass-through provisions. The registrar is also fully obligated to their accreditation contracts with ICANN (via the RAA) which includes elements such as the UDRP.

In general, the contracts will establish that the registry operator may reject a registration request, or can delete, revoke, update, suspend, cancel, or transfer a registration for violations of our anti-abuse policies. The terms in our proposed agreement will empower us to take necessary action including, but not limited to:

* Discretionary action against domain names that are not accompanied by complete and accurate information as required by ICANN Requirements and⁄or Registry Policies or where required information is not updated and⁄or corrected as required by ICANN Requirements and⁄or Registry Policies;

* Action as may be required to protect the integrity and stability of the Registry, its operations, and the TLD system;

* Action as may be required to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the Registry;

* Action as may be required to establish, assert, or defend the legal rights of the Registry or a

third party or to avoid any civil or criminal liability on the part of the Registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;

* Action as may be required to correct mistakes made by the Registry or any Accredited Registrar in connection with a registration; or

* Enforcement of Registry policies and ICANN requirements; each as amended from time to time;

* Actions as otherwise provided in the Registry-Registrar Agreement and/or the Registry-Registrant Agreement.

Below are some additional points that we will look to cover in the RRA. These clauses will enable us to enforce some additional, proactive measures to curb and deter abuse:

* We will reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

* We will reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

* We may amend or otherwise modify this policy to keep abreast of changes in consensus policy or new and emerging types of abusive behaviour in the Internet.

* Relevant language that enforces Registrars to conform with the SLAs provided for abuse cases delegated to them and provides the Registry with rights to take relevant actions in those cases.

* Relevant language for sanctions against a Registrar leading to termination with respect to repeated offences and violations of their obligations with respect to abuse mitigation.

* Relevant language that requires Registrars to provide for the following in their agreement with the Registrants
** Whois accuracy provisions
** Acceptable content and usage policy
** Sunrise policy and submission to SDRP
** UDRP
** Rights granted to the Registrar and Registry to take necessary action wrt abuse prevention including sharing information with regulatory bodies and LEA and domain takedowns where appropriate
** Indemnification
** Eligibility Restrictions and submission to ERDRP

All of the contracts above will be regularly reviewed (atleast once a year) based on the experience gained by the Registry during actual operation and any relevant changes required to mitigate abuse will be appropriately introduced in consultation with ICANN and the Registrars

4.8. ADDITIONAL MITIGATION MEASURES

Based on our experience of running a leading Registrar, we have also devised some powerful mechanisms which will prevent possible abuse, and quickly diffuse abusive domains. These mechanisms include:

4.8.1. PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.
When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer’s control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the 'Profiling and Blacklisting' process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Hotel will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

4.8.2. PROACTIVE QUALITY REVIEW

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Hotel, and encourage registrars to incorporate this practice as part of their abuse mitigation processes.

4.9. INDUSTRY COLLABORATION AND INFORMATION SHARING

Upon obtaining Registry Accreditation, we will join the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address internet identity theft, especially phishing and malware distribution. In addition, Directi coordinates with the Anti-Phishing Working Group (APWG), other DNS abuse prevention organizations and is subscribed to the NXdomain mailing list.
Directi's strong participation in the industry facilitates collaboration with relevant organizations on abuse related issues and ensures that Directi is responsive to new and emerging domain name abuses.

The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behavior in other TLDs. While presence on such lists will not directly constitute grounds for registrant disqualification, we will investigate domain names registered to those listed registrants and take appropriate action. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

5. PROMOTING AND ENSURING WHOIS ACCURACY

All registrants shall be required, via required language in every Registrar – Registrant Agreement, to provide accurate Registrar Data Directory Services, RDDS (WHOIS) contact details, and to keep those details current. Additionally, Registrars shall have direct responsibility to ensure Whois accuracy through their accreditation contracts with ICANN. Whois Data Reminder Policy or WDRP is an example of a direct Registrar⁄ICANN contractual obligation to monitor that RDDS (WHOIS) information is accurate and up to date – it includes requiring Registrars to notify their registrants at least once a year to ensure their RDDS (WHOIS) data is correct and up to date.

The threat of inaccurate Whois information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEA's rely on the integrity and accuracy of Whois information in their investigative processes to identify and locate wrongdoers.

In recognition of this, we propose that .Hotel have the following measures to promote RDDS (WHOIS) accuracy.

5.1. WHOIS INACCURACY REPORTING SYSTEM

On the abuse page of our Registry website, we will provide a web based submission service for reporting Whois accuracy issues. Each of these issues will then be resolved as per the process detailed in the previous sections.

5.2. REGULAR MONITORING & SAMPLING

Registrants of randomly selected domain names will be contacted by telephone using the provided Whois information by a member of our team in order to verify the phone number and confirm other Whois information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant who must then provide a contact number that is verified by our team. In the event that the registrant is not able to be contacted by any of the methods provided in Whois, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate Whois information and is grounds for terminating the registration agreement)

5.3. ANALYSIS OF REGISTRY DATA

We will adopt some processes to identify patterns and correlations indicative of inaccurate Whois (e.g. repetitive use of fraudulent details).

5.4. PROMOTING ACCURATE WHOIS DATA

WDRP (Whois Data Reminder Policy) implemented by ICANN at the Registrar level, mandates regular e-mail communication to registrants reminding them to keep their whois data accurate and updated. In addition, we will also identify effective mediums to remind registrants to update Whois information and inform them of the ramifications of a failure to respond to our random monthly checks. Ramifications include but are not limited to termination of the registration agreement.

5.5. ENFORCEMENT AT REGISTRAR LEVEL

Registrars will also be contractually required to promptly investigate reports of RDDS (WHOIS) accuracy submitted to them, and resolve each case within a predefined time-frame stipulated through our SLA.

For all cases where inaccuracy is confirmed, we will record the registrar from whom the domain was sourced. We will use this data to capture the ratio of inaccuracies as a percentage of total domains managed, and identify the registrars that seem to attract an abnormally high number of inaccuracy issues. We will then work with those registrars to find potential ways in which they can progressively reduce the number of whois inaccuracy incidents.

The measures to promote Whois accuracy described above strike a balance between the need to maintain the integrity of the Whois service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the Registry Operator and Registrars which aim to offer domain names to registrants in an efficient and timely manner.

Awareness among registrants that we will actively take steps to maintain the accuracy of Whois information mitigates the potential for abuse in the TLD. It deters abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

5.6. PROXY/PRIVACY PROTECTION

We have designed a policy that will maximize the legitimate use of proxy and privacy services, and will minimize use by criminals and abusers.

.Hotel will allow the use of proxy and privacy services, where permitted by ICANN policies and requirements. These services have legitimate uses. Millions of registrants use them to protect their privacy and personal data from spammers and other parties that mine zone files and RDDS (WHOIS) data.

It is undeniable that criminals also use whois proxy services, to hide their true identities. To deter that practice, our policy will require that:

* Registrants must use only a privacy/proxy service operated, contracted or owned by the domain's sponsoring registrar, and cannot use third-party proxy services unaffiliated with the domain's sponsoring registrar. This means that a domain's sponsoring registrar will always be in possession of the underlying contact data.

*.Registrars and resellers must provide the underlying registrant information to the registry operator upon request, and/or upon a legitimate law-enforcement request, within 24 hours. The registry operator will keep this data confidential, unless #3 below applies.

*Registrars and resellers must remove the proxy protection and publish the underlying registrant information in the RDDS (WHOIS) if it is determined by the registry operator and/or the registrar that the registrant has breached any terms of service, such as anti-abuse policies.

The registrar obligations outlined above shall apply with equal force to all registrations sponsored by a registrar, whether those registrations were placed directly with the registrar or through a reseller.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the abuse page of our Registry website. Individuals and organisations will be encouraged through our abuse page to report any domain names they believe violate the restriction on the availability of proxy registrations, following which appropriate action may be taken by us. Publication of these conditions on the abuse page of our Registry website ensures that registrants are aware that despite utilisation of a proxy registration

service, actual Whois information will be provided to LEA upon request in order to hold registrants liable for all actions in relation to their domain name. The certainty of Whois disclosure of domain names which draw the attention of LEA, deters those seeking to register domain names for abusive purposes.

6. CONTROLS FOR PROPER ACCESS TO DOMAIN FUNCTIONS

We realize that registrants often do not willfully use their domain names for abusive purposes, but domain names end up being compromised because of a lapse in security. Though this cannot always be controlled or mitigated by the registry, we are nevertheless committed to ensure that adequate safeguards are implemented to prevent domain names from being compromised and thereby making them prone to abuse.

6.1. MULTI-FACTOR AUTHENTICATIONAND SECURE CONNECTIVITY FOR REGISTRARS

Through the contractual agreement with the registry, registrars will be expected to develop and employ in their domain name registration business, all necessary technology and restrictions to ensure that their connection to the registry is secure. All data exchanged between the registrar's system and the registry shall be protected to avoid unintended disclosure of information. Each EPP session shall be authenticated and encrypted using two-way secure socket layer ("SSL") protocol. Registrars will also agree to authenticate every EPP client connection with the registry using both an X.509 server certificate issued by a commercial Certification Authority identified by the registry and their registrar password, disclosed only to their respective employees on a need-to-know basis. Registrars will also access the SRS Web interface by utilizing an additional two-factor authentication token. Further details on this is provided in the response to Question 24 and 25

6.2. ENFORCEMENT OF STRONG AUTHCODES

Every domain name will have a strong authorization (authinfo) code, composed of alphabets, numerals, and special characters. An inter-registrar domain name transfer will not be permitted unless the registrant provides this authorization code at the time of executing the transfer process.

6.3. NOTIFICATION FOR EVERY UPDATE

We plan to notify the domain name holder upon any update made to a domain name. The notification will be committed through email to either or both of the registrant and technical contact of the domain name.

6.4. REGISTRY LOCK

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. 'Registry locking' is a feature which allows registrants to prohibit any updates at the Registry Operator level. This service will be available programmatically via EPP, so all registrars will be able to offer it in real-time to their registrants. The feature will prevent unintentional transfer, modification or deletion of the domain name, and mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update name servers of a mission critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name. This is described in detail in our response to Question 27

6.5. AWARENESS PROGRAMS

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate and confidential. Awareness will be raised by:

* Publishing the necessary information on the Abuse page of our Registry website in the form of videos, presentations and FAQs;

* Developing and providing to registrants, resellers and Registrars Best Common Practices that describe appropriate use and assignment of domain auth info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

7. RESOURCING PLANS

7.1. PERSONNEL

Functions described herein will be performed by -
* Directi Group staff under contract with us -
** Abuse &Compliance Team
* Dispute Resolution Service Providers that are selected wrt UDRP, ERDRP and SDRP

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar. The abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:
* 1 Compliance Manager
* 1 Team Supervisor
* 4 Cyber Security Analysts
* 9 Compliance Officers

The compliance function is staffed on a 24⁄7⁄365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required. Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains across our Registrar businesses within Directi, each year we experience approximately:

* 6000 malware related abuses
* 1600 phishing abuses
* 1200 spam cases
* 600 pharmacy related abuses
* 5600 large botnet related abuse cases annually

This averages an incident rate of approximately 15,000 cases of abuse per year or 3.75 incidents per 1000 names

Since registries delegate a large portion of their abuse responsibilities to registrars, it is fair to assume that our registry's abuse incident ratio will belower than what we experience as registrars. In fact, in our case 2⁄3 categories of incidents will be delegated to the registrar, and our direct involvement is expected in only 25%-35% of all incidents. However, given our proactive approach, importance on ensuring a clean and secure namespace, and aggressive SLAs, we choose to be conservative by assuming that we will be involved in 75% of the incidents.

Based on our projections, we expect .Hotel to reach 26,715 domain names at the end of the 3rd year. Extrapolating from our current rate of 3.75 incidents per 1000 names, we can expect around 100 abuse incidents yearly and be involved in 75 (75%) of them .Including the estimated 4 RPM incidents (details in our response to Q29), brings our total projected incident count to approximately 79. This conservative estimate also accounts for the aggressive SLAs at multiple levels, law enforcement interfacing and having a single POC available at all times.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 15% of 2 compliance officers' time towards .Hotel. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 15% of their time, will have a total capacity to handle 1056 incidents annually. It is important to point out that 15% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for the TLD.

Our planning provides us redundant capacity of over 24 X in Y1, around 15.5 X in Y2 and over 12.2 X in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exists some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The abuse team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given the rapid growth rate of Directi businesses, Directi will continue to hire and maintain a sizable buffer over and above anticipated growth.

7.2. FINANCIAL CONSIDERATIONS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46 ('Q46_References: Service and Facilities Commitment Agreement'). This cost is shown in the financial answers.

This completes our response to Q28.

29. Rights Protection Mechanisms

DotHotel Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. At Directi, through our decade long experience as a domain name registrar, we have consciously strived to ensure that domain registrations through our platform do not violate the intellectual property or other rights of any person or organization.

Our experience as a domain name registrar gives us insight into the necessity and importance of rights protection, and the mechanisms that must be employed to assure it. With .Hotel, we shall leverage our experience to implement a comprehensive set of policies and procedures that will uphold intellectual property rights to the greatest possible extent.

The protection of trademark rights is a core goal of .Hotel. .Hotel will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPMs to prevent abusive registrations and rapidly take-down abuse when it does occur.

1. PREVENT ABUSIVE REGISTRATIONS

We will put into place the following measures to ensure prevention of registrations that infringe the IP rights of others

1.1 ELIGIBILITY REQUIREMENTS

.hotel will have a well defined eligibility requirements policy for domain registrations within .hotel along with a dispute resolution process (Eligibility Restrictions Dispute Resolution Process - ERDRP) to resolve potential abuse. Our Eligibility policy and process has the following impact on RPMs -
* Requires that general domain names within .hotel are registered by entities which are in the hotel or related businesses only.
* Ensures that in the scenario of a registrant or domain name that violates our eligibility criteria the same can be addressed through the ERDRP

1.1.1 ELIGIBILITY POLICY SUMMARY

This section provides salient aspects of our proposed eligibility policy. The actual policy will be drafted in line with the tenets described herein. Details regarding the implementation of these policies are provided in the next section of this response

* General Names can be registered by entities which are in the hotel or related businesses only

* The above applies to general domain names whether registered during sunrise, landrush or general availability

* Registry reserved generic domain names within .hotel maybe allocated in the future through other equitable means (including auctions) such as to registrants who can demonstrate business plans that will promote the .hotel namespace and benefit the registrants of general names within .hotel.

1.1.2 ELIGIBILITY POLICY IMPLEMENTATION

1.1.2.1 GENERATING AWARENESS

* The Eligibility policy implementation plan and ERDRP will be published on our Registry website which will be accessible and have clear links from the home page

* The policies will also be clearly communicated to potential Registrants during the registration process

1.1.2.3 CONTRACTUAL ENFORCEMENT

The following features of the Eligibility policy described above will be executed by the inclusion of corresponding clauses in our RRA, which will require inclusion in registrars' Domain Name Registration Agreements:

* The Registrant must maintain accurate contact information for a domain name

* The Registrant must agree to the Eligibility policy, and to proceedings under the ERDRP

1.2. SUNRISE PROCESS

Our sunrise registration service will provide trademark holders with atleast a 30-day priority period in which to register their trademarks as domain names.

Sunrise Timeline -
Day 1: Single sunrise round opens
Day 30: Sunrise round closes
Day 31: Sunrise allocation begins and Sunrise period ends

1.2.1. SUNRISE POLICY SUMMARY AND SDRP SUMMARY

This section provides a summary of our Sunrise Policy and SDRP. We have formulated our policies and processes based on existing guidance concerning Sunrise and TMCH provided by ICANN. Any additional guidance in the future that requires changes to our process and policies will be implemented.

Through our Sunrise Policy we will offer atleast one 30-day sunrise round in which trademark holders satisfying the Sunrise eligibility requirements proposed in the 'gTLD Applicant Guidebook' will be eligible to apply for a domain name. This sunrise period will be the first opportunity for registration of domain names in .Hotel. Trademarks upon which sunrise applications are based must meet the criteria defined in the 'gTLD Applicant Guidebook' and be supported by an entry in the TMCH.

Sunrise allocation will start at the end of the 30-day sunrise period. If one validated application is received for a domain name, the same will be allocated to the applicant in the 10-day period following the end of the sunrise period. Where multiple validated applications are received for a domain name, the name will be allocated by auction. Domain names registered during the sunrise period will have a term of 1 yr.

We will adopt a Sunrise Dispute Resolution Policy ('SDRP') to allow any party to raise a challenge on the four grounds identified in the 'gTLD Applicant Guidebook'. All registrants will be required to submit to proceedings under the SDRP. SDRP claims may be raised at any time after registration of a domain name.

1.2.2. IMPLEMENTATION

1.2.2.1. SUNRISE PRICING

We plan to charge a non-refundable Sunrise application fee or validation fee of $80 for every Sunrise application. We have arrived at the fee to offset the cost of the trademark validation and other administrative over-heads.

1.2.2.2. SUNRISE IMPLEMENTATION PLAN

1. Prior to sunrise, trademark holders should apply for inclusion of their marks in the TMCH database.
2. Our Sunrise Policy and SDRP will be published on our website.
3. A trademark holder satisfying the sunrise eligibility requirements will pay the non-refundable sunrise application fee and submit its application corresponding to its TMCH entry to a registrar along with evidence of the corresponding TMCH entry.
4. Registrars will send the sunrise applications to ARI. They will be charged the application fee at this time.
5. ARI will perform standard checks to ensure that the domain name is technically valid and hold the application for subsequent allocation.
6. Upon conclusion of the 30-day sunrise period, ARI will compile a list of applied-for names and reserve these from registration in land rush and general availability.

7. Sometime during this process ARI or the registrar (as prescribed) will identify all sunrise applications which constitute an 'Identical Match' (as defined in the 'gTLD Applicant Guidebook') with a TMCH entry and provide notice to the holders of the filing of a sunrise registration.
8. Where a single sunrise application exists for a particular domain name ARI will enable the sponsoring registrar to CREATE the domain name and we will charge the sunrise registration fee to the registrar.
9. Where multiple sunrise applications exist for a domain name, ARI will compile and communicate to a 3rd-party auction services provider appointed by us a list of competing applicants, who will be invited to participate in an auction for the domain name.
10. The auction services provider will facilitate the auction process and upon completion of the auction will notify all participants of the outcome and collect the auction payment from the winning participant.
11. Upon payment of the auction bid, the auction services provider will communicate to ARI the details of the winning auction participant and will submit the revenue collected to ARI.
ARI will validate the communication from the auction services provider and enable the sponsoring registrar to CREATE the domain name.

1.2.1.3. SDRP IMPLEMENTATION PLAN

When a domain is awarded and granted to a registrant, that domain will be available for lookup in the public WHOIS.

After a Sunrise name is awarded it will also remain under a "Sunrise Lock" status for at least 60 days. During this 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 the subject of a Sunrise Challenge. Challenged domains will remain locked until the dispute resolution provider has issued a decision, which the registry operator will promptly execute.

SDRP filings will be handled by an appropriate service provider as per ICANN guidance and policy.

1.2.1.4. IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of the Sunrise and SDRP implementation plans described above will be executed by the inclusion of corresponding clauses in our RRA, which will require inclusion in registrars' Domain Name Registration Agreements:
* By making a sunrise application the applicant agrees to purchase the domain name if that name is allocated to the applicant.
* The sunrise application fee is non-refundable.
* All sunrise applicants must submit to proceedings under the SDRP.

1.3. TRADEMARK CLAIMS SERVICE

For atleast 60 days during general availability we will offer the trademark claims service as described in the 'gTLD Application Guidebook'.

1.3.1. IMPLEMENTATION

1.3.1.1. TRADEMARK CLAIMS SERVICE IMPLEMENTATION PLAN

This process will be executed for atleast the first 60 days of general availability:
1. an applicant will make an application to a registrar for a domain name.
2. Registrars will be required to communicate land rush application information to our registry backend provider - ARI.
3. ARI or Registrars (as prescribed) will interface with the TMCH to determine whether an applied-for domain name constitutes an 'Identical Match' with a trademark in the TMCH. If an 'Identical Match' is identified, the registrar will provide to the land rush applicant a Trademark Claims Notice in the form prescribed by the 'gTLD Applicant Guidebook'. Following receipt of this notice a land rush applicant must communicate to the registrar its decision either to proceed with or abandon the registration.
4. ARI or Registrar (as prescribed) will interface with the TMCH to promptly notify relevant mark holders of the registration of a domain name constituting an 'Identical Match' to their TMCH entry.

1.3.1.2. IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our Trademark Claims Service Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:
* Registrars must comply with the TMCH as required by ICANN and the TMCH Service Provider⁄s.
* Registrars must not in their provision of the trademark claims service make use of any other trademark information aggregation, notification or validation service other than the TMCH.

* In order to prevent a chilling effect on registration, registrars must ensure that land rush applicants are not prevented from registering domain names considered an 'Identical Match' with a mark in the TMCH.
* Registrars must provide clear notice in the specific form provided by the 'gTLD Applicant Guidebook' to the prospective registrant of relevant entries in the TMCH.
* Registrars must interface with the TMCH as prescribed to relevant mark holders of the registration of a domain name constituting an 'Identical Match' to their TMCH entry.

2. ONGOING RIGHTS PROTECTION AND ABUSE PREVENTION

Below we describe ongoing RPMs which we will implement to mitigate cybersquatting and other types of abusive behaviour such as phishing and pharming.

2.1. UNIFORM RAPID SUSPENSION (URS)

The URS (Uniform Rapid Suspension) procedure is a new RPM the implementation of which is mandated in all new gTLDs. Understanding that a fundamental aim of the URS is expediency, all of the steps in our Implementation Plan below will be undertaken as soon as practical but without compromising security or accuracy.

2.1.1. IMPLEMENTATION

2.1.1.1. URS IMPLEMENTATION PLAN

1. We will provide to each URS provider an email address to which URS-related correspondence can be sent. On an ongoing basis, our compliance desk will monitor this email address for receipt of communications from URS providers, including the Notice of Complaint, Notice of Default, URS Determination, Notice of Appeal and Appeal Panel Findings.
2. We will validate correspondence from a URS provider to ensure that it originates from the URS Provider.
3. We will within 24 hours of receipt of a URS Notice of Complaint lock the domain name⁄s the subject of that complaint by restricting all changes to the registration data, including transfer and deletion of the domain name. The domain name will continue to resolve while in this locked status.
4. We will immediately notify the URS provider in the manner requested by the URS provider once the domain name⁄s have been locked.
5. Upon receipt of a favourable URS Determination we will unlock the domain name and redirect the nameservers to an informational web page provided by the URS provider. While a domain name is locked, our backend provider - ARI - will continue to display all of the WHOIS information of the original registrant except for the redirection of the nameservers and the additional statement that the domain name will not be able to be transferred, deleted or modified for the life of the registration.
6. Upon receipt of notification from the URS provider of termination of a URS proceeding we will promptly unlock the domain name and return full control to the registrant.
7. Where a default has occurred (because a registrant has not submitted an answer to a URS complaint in accordance with the 'gTLD Applicant Guidebook') and a Determination has been made in favour of the complainant, in the event that we receive notice from a URS provider that a Response has been filed in accordance with the 'gTLD Applicant Guidebook', we will as soon as practical restore a domain name to resolve to the original IP address while preserving the domain's locked status until a Determination from de novo review is notified to us.
8. We will ensure that no changes are made to the resolution of a registration the subject of a successful URS Determination until expiry of the registration or the additional registration year unless otherwise instructed by a UDRP provider.
9. We will make available to successful URS complainants an optional extension of the registration period for one additional year.

2.1.1.2. IMPLEMENTATION OF THE URS THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our URS Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:
* In the event that a Registrant does not submit an answer to a URS complaint in accordance with the 'gTLD Applicant Guidebook', registrars must prevent registrants from making changes to the WHOIS information of a registration while it is in URS default.
* Registrars must prevent changes to a domain name when a domain is in locked status to ensure that both the Registrar's systems and Registry's systems contain the same information for the locked domain name.
* Registrars must not take any action relating to a URS proceeding except as in accordance with a validated communication from us or a URS provider.

2.2. UDRP

The UDRP (Uniform Domain Name Dispute Resolution Policy) is applicable to domain name registrations in all new gTLDs. It is available to parties with rights in valid and enforceable trade or service marks and is actionable on proof of all of the following three grounds:
1. the registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
2. the registrant has no rights or legitimate interests in respect of the domain name.
3. the registrant's domain name has been registered and is being used in bad faith.

The remedies offered by the UDRP are cancellation of a domain name or transfer of a domain name registration to a successful UDRP claimant.

2.2.1. IMPLEMENTATION

2.2.1.1. UDRP IMPLEMENTATION PLAN

We have two responsibilities in order to facilitate registrars' implementation of the UDRP -
1. Our backend provider – ARI - will maintain awareness of UDRP requirements and be capable of taking action when required and sufficiently skilled and flexible to respond to any changes to UDRP policy arising from future consensus policy reviews.
2. We will provide EPP and the SRS web interfaces to enable registrars to perform required UDRP functions in accordance with the Policy on Transfer of Registrations between Registrars.

2.2.1.2. IMPLEMENTATION OF THE UDRP THROUGH CONTRACTUAL RELATIONSHIPS

The UDRP is applicable to domain name registrations in all new gTLDs by force of a contractual obligation on Registry Operators to use only ICANN-accredited registrars, who in turn are contractually required to incorporate the UDRP in their Domain Name Registration Agreements.

3. ADDITIONAL RIGHTS PROTECTION MECHANISMS

The protection of trademark rights is a core goal of .Hotel. Our Right Protection Mechanisms, policies and procedures go significantly above and beyond the minimum mandated RPMs to prevent abusive registrations, rapidly take-down abuse when it occurs, and foster a clean namespace for .Hotel

This section describes several other RPMs that .Hotel will implement that exceed the minimum requirements for RPMs and align with our goal of creating a namespace that provides maximum protection to trademark holders.

3.1 ERDRP

.hotel will have a well defined eligibility requirements policy for domain registrations within .hotel along with a dispute resolution process (Eligibility Restrictions Dispute Resolution Process - ERDRP).

As described in Q28 and above in section 1, domain names that violate the eligibility requirements will be dealt with via a dispute resolution process administered by a dispute resolution provider.

3.2. OPTIONAL TRADEMARK DECLARATION

This is a unique feature of our .Hotel. During General Availability, we will continue to make available, the EPP Trademark extension fields that are provided during sunrise. Registrants will be able to specify their IPR details against their domain names even after sunrise. The fields will include – word mark, registration number, applied date, registration date, jurisdiction, class. These fields will be editable by the Registrant and visible in Whois.

The ability for a Registrant to voluntarily declare Trademark data even during general availability will reduce potential confusion amongst mark holders and the general public and reduce unnecessary UDRP procedures.

3.3. PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.
When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer's control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the 'Profiling and Blacklisting' process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Hotel will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

3.4. PROACTIVE DOMAIN QUALITY ASSURANCE

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Hotel, and encourage registrars to incorporate this practice as part of their abuse mitigation processes.

3.5. INDUSTRY COLLABORATION

3.5.1. ACTIVE INVOLVEMENT WITH SECURITY AGENCIES

In order to mitigate abuse of domain names on our registrar business, our abuse team has active involvement in helping security vendors and researchers fight domain abuse. They provide us a constant feed of abuse instances and help us identify domain names involved in activities like phishing or pharming. Some of the prominent organizations we work with include PhishLabs (phishing), LegitScript (illegal pharmaceutical distribution), Artists Against 419 (financial scams), Knujon (spam) etc. We will leverage these relationships to ensure oversight for all domain names registered within .Hotel.

3.5.2. APWG REVIEW

Every six months, the Anti-Phishing Working Group (APWG) publishes its latest Global Phishing Survey [See http://www.apwg.org/resources.html#apwg]. This study contains an analysis of phishing per TLD. We will review the performance of our anti-abuse program against the APWG reports, and other metrics created by the security community. We will work closely with APWG to combat phishing within .Hotel

3.5.3. MESSAGE OF ZERO TOLERANCE

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

The Directi Group has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Hotel. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in violation of our policies are suspended rapidly, this will directly result in discouraging abusive registrations and creating a clean namespace. While following this path will mean a higher compliance and abuse vigilance cost for us, we believe this effort will pay us long term rewards through abusers keeping away and .Hotel becoming recognized as a reputable namespace.

4. REDUCING PHISHING AND PHARMING

All of the measures we have described in the preceding sections significantly reduce phishing and pharming within .Hotel. These include URS, UDRP and Eligibility Restrictions.

Over and above this our coordination with APWG, Industry Collaboration, Profiling and Blacklisting processes and Proactive measures described in Section 3 above will go a long way in ensuring a clean namespace for .Hotel and considerably reduced phishing and pharming activities.

5. PREVENTING TRADEMARK INFRINGEMENT IN OPERATING THE REGISTRY

We take seriously our responsibilities in running a registry and we understand that while offering a sunrise registration service and the trademark claims service during start-up of our TLD and the URS and UDRP on an ongoing basis serves to minimise abuse by others, this does not necessarily serve to minimise trademark infringement in our operation of the TLD. This responsibility is now clearly expressed and imposed upon registries through the new Trademark PDDRP [Post-Delegation Dispute Resolution Procedure], which targets infringement arising from the Registry Operator's manner of operation or use of its TLD.

Whilst we will as required under the Registry Agreement agree to participate in all Trademark PDDRP procedures and be bound by the resulting determinations, we will also have in place procedures to identify and address potential conflicts before they escalate to the stage of a Trademark PDDRP claim.

5.1. IMPLEMENTATION

1. We will notify to the Trademark PDDRP provider⁄s contact details to which communications regarding the Trademark PDDRP can be sent.
2. We will publish our Anti-Abuse Policy on a website specifically dedicated to abuse handling in our TLD.
3. Using the single abuse point of contact discussed in detail in our response to Q28, a complainant can notify us of its belief that that one or more of its marks have been infringed and harm caused by our manner of operation or use of our TLD
4. We will receive complaints submitted through the single abuse point of contact.
5. The Compliance Team will acknowledge receipt of the complaint and commence investigation of the subject matter of the complaint and good faith negotiations with the complainant in accordance with the 'gTLD Applicant Guidebook'.
6. On an ongoing basis, our Compliance Team will monitor the email address notified to the Trademark PDDRP provider⁄s for all communications from the Trademark PDDRP provider, including the threshold determination, Trademark PDDRP complaint, complainant's reply, notice of default, expert panel determinations, notice of appeal and determinations of an appeal panel.
7. In the event that a complaint cannot be resolved and a Trademark PDDRP claim is made, we will do the following:
* file a response to the complaint in accordance with Trademark PDDRP policy section 10 (thus avoiding, whenever possible, a default situation).
* where appropriate, make and communicate to the Trademark PDDRP provider decisions regarding the Trademark PDDRP proceeding, including whether to request a three-person Trademark PDDRP Expert Panel, request discovery, request and attend a hearing, request a de novo appeal, challenge an ICANN-imposed Trademark PDDRP remedy, initiate dispute resolution under the Registry Agreement, or commence litigation in the event of a dispute arising under the Trademark PDDRP.
* where appropriate, undertake discovery in compliance with Trademark PDDRP policy section 15, attend hearings raised under section 16 if required, and gather evidence in compliance with sections 20.5 and 20.6.
8. We will upon notification of an Expert Panel finding in favour of the Claimant (Trademark PDDRP policy section 14.3), reimburse the Trademark PDDRP Claimant.
9. We will implement any remedial measures recommended by the expert panel pursuant to Trademark PDDRP policy and take all steps necessary to cure violations found by the expert panel and notified by ICANN.

6. RESOURCING PLANS

6.1. PERSONNEL

Functions described herein will be performed by -
* Directi Group Abuse and Compliance team under contract with us -
** Overseeing Sunrise process
** URS
** Abuse complaints concerning RPM
* ARI's backend Registry
* Service Providers that are selected wrt TMCH, UDRP, URS, ERDRP and SDRP
* Director of Technology at .Hotel & Account Management staff at .Hotel
** Overseeing Sunrise process
** Communication of the sunrise process to Registrars

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar business. The Rights protection and abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:
* 1 Compliance Manager
* 1 Team Supervisor
* 4 Cyber Security Analysts
* 9 Compliance Officers

The compliance function is staffed on a 24⁄7⁄365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required. Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains as a Registrar, we experience approximately the following incidents per year:
* UDRP Cases - 200
* Other RPM incidents - 20 cases

This averages an incident rate of approximately 220 cases of abuse per year or 0.055 incidents per 1000 names. Given that this is based on a more mature base of names, it would be prudent to assume a higher rate of activity for .Hotel. Based on our experience we have assumed the increase in activity rate to be three fold (300% of the current rate) and increase it to 0.165 per 1000 names.

Based on our projections, we expect .Hotel to reach 26,715 domain names at the end of the third year. Extrapolating from our estimated rate of 0.165 incidents per 1000 names, we can expect around 4 incidents yearly. Including the estimated 75 Abuse incidents that the registry will be involved in (details in our response to Q28), brings our total projected incident count to approximately 80.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 15% of two compliance officers' time towards .Hotel. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 15% of their time, will have a total capacity to handle 1056 incidents annually which is more than adequate for the Registry. It is important to point out that 15% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for TLD.

Our planning provides us redundant capacity of over 24 X in Y1, around 16 X in Y2 and over 12 X in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exist some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The Abuse and Compliance team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given our rapid growth rate and business expansion plans, we will continue to hire and maintain a sizable buffer over and above anticipated growth.

6.2. FINANCIAL COSTS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q29.

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

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI

please see the attachment 'Q30a – ARI Background & Roles.pdf'. This response describes Security as implemented by ARI under direction from us taking into account any specific needs for this TLD.

1. SECURITY POLICY SUMMARY

ARI operates an ISO27001 compliant Information Security Management System (ISMS) for Domain Name Registry Operations; see attachment 'Q30a – SAI Global Certificate of Compliance.pdf'. The ISMS is an organisation-wide system encompassing all levels of Information Security policy, procedure, standards, and records. Full details of all the policies and procedures included in the ISMS are included in the attachment to Question 30b.

1.1 THE ISMS

ARI's ISMS's governing policy:
* Defines the scope of operations to be managed (Domain Name Registry Operations).
* Designates the responsible parties (COO, CTO and Information Security Officer) for governance, Production Support Group for implementation and maintenance, and other departments for supporting services.
* Requires a complete Risk Assessment (a developed Security Threat Profile for the Service – in this case registry services for the TLD – and a Risk Analysis tracing threats and vulnerabilities through to Risks) and Risk Treatment Plan (each major risk in the Risk Assessment references the Statement of Applicability indicating controls to be implemented, responsible parties, and the effectiveness metrics for each).
* Includes a series of major sub policies governing security, which include but are not limited to:
 ** ICT acceptable use policy and physical security policies.
 ** PSG Security Policy which outlines the registry operations policies, the management of end-user devices, classification of networks and servers according to the classification of information they contain, networking, server & database configuration and maintenance guidelines, vulnerability and patch management, data integrity controls, access management, penetration testing, third party management, logging and monitoring, and cryptography.
* Requires ongoing review:
 ** Of risks, threats, the Risk Treatment Plan, client requirements and commitments, process and policy compliance, process and policy effectiveness, user etc.
 ** Regular internal and external penetration testing & vulnerability scanning.
 ** Ad-hoc review raised during normal operations, common sources being change management processes, scheduled maintenance or project debriefs, and security incidents.
 ** Yearly review cycle which includes both internal and external audits, including external surveillance audits for compliance.
 ** Additional yearly security controls assessment reviews, which include analysis of the security control implementations themselves (rather than compliance with any particular standard).
 ** At 24 month intervals, external penetration testing of selected production services.
 ** Periodic ISO reaccreditation
ARI's ISMS encompasses the following ARI standards:
* Configuration standards for operating systems, networking devices and databases based on several key publications, including those released by NIST (e.g. SP800-123, SP800-44v2, SP-800-40, SP800-41) and the NSA, staff testing and experience, and vendor supplied standards.
* Security Incident Classification, which identifies the various classifications of security incidents and events to ensure that events that qualify as security incidents.
* Information Classification and Handling which specifies the information classification scheme and the specific requirements of handling, labelling, management and destruction for each level of classification.

1.2 SECURITY PROCESSES

Processes are used to implement the policies. These include, but are not limited to:

1.2.1 CHANGE MANAGEMENT

This includes change management and its sub-processes for access management, software deployment, release of small changes and scheduled maintenance. This process includes:
* The classification of changes and the flow into sub processes by classification.
* The release and deployment process for change control into production environments, outlining peer review, testing steps, approval points, checklist sets, staging requirements and communication requirements.
* The software release and deployment process with its specific testing and staged rollout requirements.
* The scheduled maintenance process and its various review points.

1.2.2 INCIDENT MANAGEMENT

This includes incident management process and its sub-process for unplanned outages. These outline:
* How incidents are managed through escalation points, recording requirements, communication requirements etc.
* The unplanned outage procedure which applies directly to situations where the registry itself or other critical services are unexpectedly offline.

1.2.3 PROBLEM MANAGEMENT

The goal of problem management is to drive long term resolution of underlying causes of incidents. This process centres on finding and resolving the root causes of incidents. It defines escalation points to third parties or other ARI departments such as Development, as well as verification of the solution prior to problem closure.

1.2.4 SECURITY INCIDENT MANAGEMENT

This process deals with the specific handling of security incidents. It outlines the requirements and decision points for managing security incidents. Decision points, escalation points to senior management and authorities are defined, along with evidence-gathering requirements, classification of incidents and incident logging.

1.2.5 ACCESS MANAGEMENT

This process handles all access changes to systems. HR must authorize new users, and access changes are authorized by departmental managers and approved by the Information Security Officer. When staff leave or significantly change roles, a separation process is followed which ensures all access that may have been granted during their employment (not just their initially granted access) is checked and where appropriate, revoked.
Finally, quarterly review of all access is undertaken by the ISO, reviewing and approving or rejecting (with an action ticket) as appropriate.

2. ARI's SECURITY INFRASTRUCTURE SOLUTIONS

ARI has developed a layered approach to IT security infrastructure. At a high level, some of the layers are as follows:
* DDoS countermeasures are employed outside ARI networks. These include routing traps for DDoS attacks, upstream provider intervention, private peering links and third party filtering services.
* Routing controls at the edge of the network at a minimum ensures that only traffic with valid routing passes into ARI networks.
* Overprovisioning and burstable network capabilities help protect against DoS and DDoS attacks.
* Network firewalls filter any traffic not pre-defined by network engineering staff as valid.
* Application layer firewalls then analyse application level traffic and filter any suspicious traffic. Examples of these would be an attempt at SQL injection, script injection, cross-site scripting, or session hijacking.
* Server firewalls on front-end servers again filter out any traffic that is not strictly defined by systems administrators during configuration as valid traffic.
* Only applications strictly necessary for services are running on the servers.
* These applications are kept up-to-date with the latest security patches, as are all of the security infrastructure components that protect them or that they run on.
* ARI infrastructure is penetration-tested by external tools and contracted security professionals for vulnerabilities to known exploits.
* ARI applications are designed, coded and tested to security standards such as OWASP and penetration-tested for vulnerabilities to common classes of exploits by external tools and contracted security professionals.
* ARI configures SELinux on its production servers. Specific details of this configuration is confidential; essentially any compromised application is extremely limited in what it can do.
* Monitoring is used to detect security incidents at all layers of the security model. Specifically:
  ** Network Intrusion Detection systems are employed to monitor ARI networks for suspicious traffic.
  ** ARI maintains its own host-based Intrusion Detection system based on tripwire, which has now undergone four years of development. Specific details are confidential, but in summary, the system can detect any unusual activity with respect to configuration, program files, program processes, users, or network traffic.
  ** More generic monitoring systems are used as indicators of security incidents. Any behaviour outside the norm across over 1,100 individual application, database, systems, network and environmental checks is investigated.
* Capacity management components of the monitoring suite are also used to detect and classify security incidents. Some examples are:
 ** Network traffic counts, packet counts and specific application query counts.
 ** Long term trend data on network traffic vs. specific incident windows.

** CPU, Storage, Memory and Process monitors on servers.
* A second layer of hardware firewalling separates application and middle tier servers from database servers.
* Applications only have as much access to database information as is required to perform their function.
* Finally, database servers have their own security standards, including server-based firewalls, vulnerability management for operating system and RDBMS software, and encryption of critical data.

2.1 PHYSICAL SECURITY INFRASTRUCTURE

ARI maintains a series of physical security infrastructure measures including but not limited to biometric and physical key access control to secured areas and security camera recording, alarm systems and monitoring.

3. COMMITMENTS TO REGISTRANTS

We commit to the following:
* Safeguarding the confidentiality, integrity and availability of registrant's data.
* Compliance with the relevant regulation and legislation with respect to privacy.
* Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
* Maintaining a best practice information security management system that continues to be ISO27001 -compliant.
* Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
* That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.
** That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
** A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
* That emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

4. AUGMENTED LEVEL OF SECURITY

This TLD is a generic TLD and as such requires security considerations that are commensurate with its purpose. Our goal with this TLD is to provide registrants with adequate protections against unauthorized changes to their names, without making the registration process too onerous and thus increasing costs.
The following attributes describe the security with respect to the TLD:
* ARI, follows the highest security standards with respect to its Registry Operations. ARI is ISO 27001 certified and has been in the business of providing a Registry backend for 10 years. ARI have confirmed their adherence to all of the security standards as described in this application.
* Registrant will only be permitted to make changes to their domain name after a authenticating to their Registrar.
* Registrants will only be able to access all interfaces for domain registration and management via HTTPS. A reputed digital certificate vendor will provide the SSL certificate of the secure site.
* Registrar identity will be manually verified before they are accredited within this TLD. This will include verification of corporate identity, identity of individuals involved ⁄ mentioned, and verification of contact information
* Registrars will only be permitted to connect with the SRS via EPP after a multi-factor authentication that validates their digital identity. This is described further ahead.
* Registrars will only be permitted to use a certificate signed by ARI to connect with the Registry systems. Self-signed certificates will not be permitted.
* The Registry is DNSSEC enabled and the TLD zone will be DNSSEC enabled. This is described in detail in our response to question 43.
* Registrar access to all Registry Systems will be via TLS and secured with multi-factor authentication. This is described in detail in our responses to Question 24 and Question 25.
Where these requirements put controls on Registrars these will be enforced through the RRA.

5. RESOURCES

This function will be performed by ARI. The following resources are allocated to performing the tasks required to deliver the services described:
* Executive Management Team (4 staff)
* Production Support Group (27 staff)
ARI has ten years' experience designing, developing, deploying, securing and operating critical

Registry systems, as well as TLD consulting and technology leadership.
As a technology company, ARI's senior management are technology and methodology leaders in their respective fields who ensure the organization maintains a focus on technical excellence and hiring, training and staff management.
Executive Management are heavily involved in ensuring security standards are met and that continued review and improvement is constantly undertaken. This includes the:
* Chief Operations Officer
* Chief Technology Officer
A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q30a – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system.

Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 26,715 domains, 0.05% of these resources are allocated to this TLD. See attachment 'Q30a – Registry Scale Estimates & Resource Allocation.xlsx' for more information.

The Production Support Group is responsible for the deployment and operation of TLD registries.

ARI employs a rigorous hiring process and screening (Police background checks for technical staff and Australian Federal Government 'Protected' level security clearances for registry operations staff).

This completes our response to Q30(a).

crowell moring

Annex 7.

New gTLD Application Submitted to ICANN by: HOTEL Top-Level-Domain S.a.r.l

String: hotel

Originally Posted: 13 June 2012

Application ID: 1-1032-95136

Applicant Information

1. Full legal name

HOTEL Top-Level-Domain S.a.r.l

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Contact Information Redacted

5. If applicable, website or URL

http://www.dothotel.info

Primary Contact

6(a). Name

Mr. Johannes Lenz-Hawliczek

6(b). Title

Chief Executive Officer

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

Contact Information Redacted

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Ms. Katrin Ohlmer

7(b). Title

Chief Executive Officer

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

Contact Information Redacted

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Societe a responsabilite limitee (S.a.r.l.)

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

The Societe a responsabilite limitee (Limited Liability Company) is defined in the Loi du 10 aout 1915 concernant les societes commerciales of the Grand Duchy of Luxembourg. http://www.legilux.public.lu/leg/a/archives/1915/0090/index.html. The company register is the Registre de Commerce et des Societes, Luxembourg.

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

Attachments are not displayed on this form.

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

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

Not Applicable.

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

Not Applicable.

Applicant Background

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

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

Johannes Lenz-Hawliczek	Chief Executive Officer
Katrin Ohlmer	Chief Executive Officer

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

Afilias Limited	Not Applicable
HOTEL Top-Level-Domain GmbH	Not Applicable

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

Applied-for gTLD string

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

hotel

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.

Hotel Top-Level-Domain S.a.r.l. anticipates the introduction of this TLD without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:
- The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
- The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
- There are no new standards required for the introduction of this TLD;
- No onerous requirements are being made on registrars, registrants or Internet users, and;
- The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this 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.

Mission and Purpose

The .hotel top-level domain is intended exclusively to serve the global Hotel Community and is designed to help solving existing challenges in a strongly growing online hotel business. It will provide verified, meaningful and easily recognizable domains to the Hotel Community.

The Community for the .hotel top-level domain (the "Hotel Community") consists of entities that are hotels, operate hotels or represent hotels through an association. This Hotel Community intends to use .hotel domain names for their presentation, communication and commerce, and⁄or promote the hotel community online.

For this reason, the eligible registrants are limited to the following Hotel Community categories:

- Hotels
- Hotel chains

- Hotel associations

There are two primary challenges the Hotel Community faces which this TLD addresses: discoverability and profitability. The .hotel top-level domain supports the Hotel Community's strengths and enhances its worldwide presentation on the Internet for the benefit of the whole community – from single hotels to their representations – through a clear, identifiable domain. This discoverability leads to direct contacts from potential hotel customers, which will reduce dependence on third-party booking portals and increase direct bookings. This benefit will result in increased margins for the Hotel Community and better prices for hotel customers.

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

i.

Speciality – An integrally connected namespace

In our vision, the .hotel top-level domain becomes the essential name space for the communication and interaction of all participants of the global Hotel Community with their target groups like Internet users, the media and suppliers. By becoming the essential source for community members and their customers, the .hotel namespace integrally connects them on the Internet.

Reputation – A secure and trustworthy namespace
For hotel customers, .hotel will mean security, reliability, trust and credibility. The verification of each domain name ensures that only eligible entities can register a .hotel domain, therefore Internet users can rest assured that services offered under .hotel domains are only from hotels and not fake services from non-community members. This is a security and service level that is demanded by the global Hotel Community and which will contribute towards a very positive reputation of .hotel.

An intuitive and memorable namespace

Domain names under .hotel are descriptive, precise and create identity for hotels and hotel associations. It enables suppliers and enquirers to come together in a more intuitive manner than today. This is a speciality that has rarely been seen in existing top-level domains, but will become a standard in future top-level domains.

ii.

Competition - Better prices through enhanced options for the Hotel Community

With .hotel, community members will be enabled to choose from a wide pool of contextually relevant domain names and register those which best suit their communication needs. As an addition to gTLDs, ccTLDs and future gTLDs, .hotel will be an ideal supplement to existing and new TLDs. With a bigger choice between TLDs, hotels will experience a more competitive pricing for suitable domain names. Hotels will have numerous options when registering a domain because .hotel opens up a completely vacant namespace where all domain names are still available. Competition also emerges from the fact that .hotel domains offer added values for the target group that no other TLD can offer by the .hotel extension.

Differentiation - The verification makes the difference

The .hotel concept strictly limits the eligible registrants to hotels and their

associations, thus creating an exclusive, trusted namespace for the hotel industry worldwide. The .hotel TLD will have a reputation as strong and credible as the hotel brands of the Community it is serving.

Prosperous and promising namespace

This environment creates new business opportunities and fosters the development of innovative services for the benefit of the global hotel community and its participants. With .hotel domains, the global Hotel Community will have the ability to enhance their search engine rankings by delivering more relevant search results. This will benefit in more direct bookings on their respective .hotel websites and increase their position in the global hotel booking market. From a user perspective, potential hotel guests will have a quicker and easier way to find accommodations from legitimate lodging providers.

Innovation

We are planning to support the Hotel Community by innovative domain name connected services such as making websites more easy accessible for mobile devices, offering directory services and search engine optimization.

With a .hotel domain, the Hotel Community has a powerful tool to increase their margins by reducing dependency on external booking portals and increasing their direct bookings. The new .hotel domain names will be suitable for search engines and other forms of communication. Due to verification of domain names, .hotel creates more trust for hotel customers; combined with the ease of search, .hotel offers an innovative approach to supporting the booking needs of its Community.

Another innovation in .hotel is a rights protection mechanism that includes a special focus on securing trademark rights of the Hotel Community.

iii.
Users will understand that in the .hotel namespace only verified hotels can register their names, thus eliminating the potential for fraud and phishing in that area. The verification also provides consumer confidence as they can be certain they are finding and possibly booking with a legitimate hotel, or working with an established hotel association.

iv.

The .hotel top-level domain is designed to serve the hotel industry worldwide.

The term “HOTEL” is clearly defined based on the norm ISO 18513, 2.2.1: “Establishment with reception, services and additional facilities where accommodation and in most cases meals are available.” .Hotel policy is based on this definition.

.hotel second-level domain names are initially restricted to the narrow category of hotels and their organizations (Registrants) as defined by ISO 18513. Therefore, the registration of .hotel domains shall be exclusively limited to registrants from a logical alliance of the hotel industry including:

1. Individual Hotels
2. Hotel Chains
3. Hotel Marketing organizations representing members from 1. and⁄or 2.
4. International, national and local Associations representing Hotels and Hotel Associations representing members from 1. and⁄or 2.
5. Other Organizations representing Hotels, Hotel Owners and other solely Hotel related organizations representing on members from 1. and⁄or 2.

Registrant verification will be based on existing, established membership lists and other data in public industry directories.

There will be two types of .hotel domain name selection policies:

1. Domain Name selection restrictions that emerge from ICANN policies and contracts; and
2. Domain Name selection restrictions that emerge solely from the Registry's delegated authority.

The core principle of name selection is that the first registrant eligible for a domain name registration will be entitled to register that domain name. The date and time of completion of all registration requirements and registrant eligibility verification data, following completion will determine the applicant's order of priority. Any domain name that is not registered by reason of the ineligibility of the applicant will be available for registration by any eligible party.

Domain Names available for registration

No Limitation - Any applicant that is eligible will be entitled to register any domain name that is not reserved or registered at the time of their registration submission through an ICANN accredited registrar.

No Limitation in Number - Registrants are not limited in the number of domain names they may register.

Registrant Representations - The registration application and registrant agreement will contain positive representations from the registrant that they are entitled to the domain name(s) they are or have registered. Breach of such representation will allow the Registry to take-down ineligible domain names at any time.

Content and Use Restrictions - The Registry has in its discretion developed restrictions on the content and use of any domain name. Such restrictions apply to any domain name registration that occurs after such restrictions come into effect.

Each domain name must, within one year following the date of registration, and thereafter throughout the term of the domain name registration, be used as the domain name for a website displaying hotel community related content relevant to the domain name, or in such other manner (such as email) that the Registry may approve after review. Domain names used as contemplated above may resolve directly to the relevant website or be forwarded or redirected to another domain name displaying hotel content relevant to the domain name.

Restrictions may include, but are not limited to, a requirement to develop a website that uses the registered domain name, to ensure that each registered domain name resolves to a working website, or to ensure that each website using a registered domain name, or redirected from a registered domain name presents content related to the registered .hotel domain name.

The .hotel Registry will, from time to time in its sole discretion or upon evidence or advice, but at least once a year, conduct continuing or recurring audits of domain names registered to ensure continued compliance with these requirements. Failure to comply will result in a notice providing 20-days to comply. Non-compliance following such a notice period may result in take-down of the relevant domain name, at the discretion of the Registry.

Equivalent Rights

The Registry will accept registration requests on a "first-come, first-served" basis. In the event an application does not meet the requirements of the Registry Policies, then such .hotel domain names will remain in the general pool of available names.

Names including the string “hotel” - Where the applicant’s held or used names include a name including the word “hotel” in any position (e.g. ABC Hotel, or ABC XYZ Hotel, or Hotel ABC), the Registry will accept during the Sunrise phase or later registration of a name in which the string “hotel” is formed at the first level and the remainder of the name is formed at the second level (e.g. “Hotel ABC” may register the name “ABC.hotel”, subject to limitations that may be placed on the string at the second level as a result of the Registry’s policy on ICANN Names and other Names.

Third-level Names

All registrants will have the right to use any name at the third level, where they hold the right to the second level name (e.g. where aaa.hotel is held, the registrant will be entitled to use bbb.aaa.hotel, ccc.aaa.hotel etc.), with the exception of 2-letter country codes. Such third level usage is not managed by the Registry.

Registrants are entitled to sell or allocate third level names to entities that are not owned or controlled by the registrant, as long as they fulfil the requirements of eligibility. For example, a hotel chain is entitled to allocate third level names to its local hotels.

It is the role of the .hotel Registry to assure and control the registrant’s eligibility to register a domain name to guarantee the community aspect and integrity of the .hotel name space and to avoid disputes. The .hotel Registry anticipates that disputes over the registrant’s eligibility will be minimal within the Hotel Community. Nevertheless it has put in place an adequate procedure to assist the hotel community’s registrants in dealing with denials of registrant’s eligibility in a way that supports community needs and values. The .hotel Registry’s informal denial procedures will not super-cede any formal dispute procedures.

Registrant Eligibility Verification

Any domain name registered under the terms set out above is subject to a subsequent registrant eligibility verification process which will start immediately after the registration process begins. Registrant eligibility verification will occur after domain name registration but before the registered domain name can be used for web services and protocols like email, website, and FTP. This is to avoid mass fraudulent domain name registrations.

Registrant data supplied for registrant eligibility verification purposes will be held and used by the Registry for eligibility verification purposes only, based on European data protection laws. Registrant eligibility verification requires a review by an applicable organization or by the Registry (reviewer). The registrant eligibility verification process starts with the Registry evaluation of each domain registration request. For evaluation purposes, industry databases will be used, like hotel association databases or other electronically available databases. Within 48 hours after registration begins, the registry will provide the evaluation result to the registrar.

In the event the registry cannot verify eligibility with the .hotel requirements, the potential registrant may be required to provide further evidence supporting their eligibility. Once reviewed, the registry will confirm or deny the registration. Confirmation will be conveyed to the registrar by email. In the event of denial of the registrant’s registration, the domain name is taken-down in the Registry’s discretion. A denial of registrant’s eligibility will be recorded against the registrant’s domain name and they will not be entitled to register a domain name until their circumstances have changed such that their registrant eligibility is confirmed in the required manner.

Registrant eligibility verification reviews may occur following domain name registration and where a registrant is found to be ineligible subsequent to

registration of a domain name(s), and such ineligibility is due to mistake or error on the part of the registrant.

The registry confirms registrant's eligibility for up to one year and the registrant may be reviewed annually or at any other time by the Registry to ensure that registrant's eligibility data have not changed in the prior period and that they continue to be eligible. If any change has occurred the registrant at any time may re-submit their registrant's eligibility data and it may be reviewed and confirmed as for initial registrant eligibility verification.

v.
The use of proxy and privacy services to protect the privacy or confidential information of registrants or users will be not allowed. Reasons are legal entities such as a the eligible registrants cannot demand privacy under most legislation and that proxy and privacy services would not allow a proper validation and a public visibility of accurate Whois data inline with the eligibility criteria.

vi.
Our concept for .hotel has been carefully developed in close cooperation with the global Hotel Community and its most important trade associations. Among those are many individual hotels, hotel chains, the International Hotel & Restaurant Association (IH&RA) which is the only representative of the hotel industry today accredited by the United Nations and the only global hotel association; HOTREC, which is the European hotel association based in Brussels; the American Hotel & Lodging Association in Washington, D.C.; and China Hotel Association (CHA). Managing Director Johannes Lenz-Hawliczek is also a member of the Board of Directors of the IH&RA.

Since 2008 our cooperation with the global hotel industry included numerous talks, presentations and discussions with leading representatives of the global hotel industry. Our outreach efforts took us to Malaysia, Thailand, China, Singapore, United Kingdom, Switzerland, Germany, Luxembourg, Belgium, the United States, Austria, Nepal, India, Serbia and Bulgaria. We also networked with representatives from Argentina, Spain, Italy, Macedonia, Montenegro, Greece, Croatia, India, Turkey, Jordan, Syria, Peru, Australia and South Korea. We attended important industry events to liaise and present the concept for .hotel to our partners from the global hotel industry.
In the 4th quarter of 2010 we started to invite Hotel Community members to join the .hotel Advisory Board, which we finally set up in March 2011. The role of Advisory Board is to advise, support and make recommendations to HOTEL Top-Level-Domain Sarl and its management. The international composition of the .hotel Advisory Board is designed to ensure that the interests of the global hotel community are being represented in a balanced way.

The board members each represent significant parts of the global hotel community, with one member representing the domain name business. Its members are Dr Ghassan Aidi, President of the International Hotel & Restaurant Association IH&RA; Joe McInerney, President and CEO of the American Hotel & Lodging Association AH&LA; Nancy Johnson, Executive Vice President of Carlson Hotels Worldwide and Chairperson of AH&LA; Markus Luthe, member of the executive committee of the European hotel association HOTREC (Hospitality Europe), and Philipp Grabensee, Chairman of the Board of Afilias for the domain name industry.

In 2012 we will continue and intensify our communication efforts to our community, with planned attendance of the most important industry events and an increase in media releases.

One example is a comment the CEO of the German hotel association, Markus Luthe, submitted to the major industry news site TNOOZ in January. In it, he laments the dependence on third party sales channels such as Expedia or booking.com hotels have gotten themselves into, bringing about an increasing loss of sales

margins across the industry due to the commissions that have to be paid to these actors. One way to improve this situation for hotels is in Mr Luthe's view for hotels to increase their share of direct bookings with the aid of "industry initiatives such as .hotel", among others.

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

Registry Reserved capital cities names

The Registry will set aside all capital cities' names. These names can be released by the Registry upon consultation with the community and the Advisory Board and registered by eligible community members.

Registry Reserved geographic names

The Registry will set aside certain geographic names. These names will be released by the Registry and can be registered by eligible community members.

Registry Reserved Domain Names for the Hotel industry associations and duties

The Registry will set aside a group of domain names that will be used by the hotel industry associations including their names, abbreviations of names and duties. These names can be released by the Registry upon request and registered by eligible community members.

Community Reserved Domain Names for major Hotel industry brands

The Registry will set aside a list of domain names that will be reserved for the 325 major hotel industry brands including sub-brands. Cut-off date for this list is September 2011. These names can be released by the Registry upon request of the brand concerned and registered by eligible community member brand. This list was decided upon in close cooperation with the Advisory Board of .hotel and is based on the annual ranking of the 325 largest hotel companies worldwide.

Registry Reserved generic Domain Names

The Registry will set aside a group of generic domain names that will be reserved for the hotel industry and can be registered by eligible community members.

Disputed Domain Names

The Registry may set aside during regular operations domain names that are being reviewed under dispute resolution procedures. These domain names may become available for registration after the dispute is concluded.

i.

All available .hotel domain names will be registered on a "first-come, first-serve" basis. Reserved names may be allocated on a "first-come, first-served" basis or via other mechanisms like auction or tender.

ii.

HOTEL Top-Level-Domain Sarl will have fair and reasonable wholesale prices that have been vetted with the Community and Registrars worldwide.

iii.

.Hotel domains will be available through accredited registrars who will be provided non-discriminatory access to registry services. The initial domain registrations for .hotel domain will be for periods of one to ten years at the discretion of the registrar.

The reserved names for auction will have discreet pricing.

HOTEL Top-Level-Domain Sarl reserves the right to reduce pricing for promotional purposes in a manner available to all accredited registrars. Registry Operator reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. Registry Operator will provide reasonable notice to the registrars of any approved price change.

Community-based Designation

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

Yes

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

The .hotel namespace will exclusively serve the global Hotel Community.

The string "Hotel" is an internationally agreed word that has a clear definition of its meaning:

According to DIN EN ISO 18513:2003, "A hotel is an establishment with services and additional facilities where accommodation and in most cases meals are available."

Therefore only entities which fulfil this definition are members of the Hotel Community and eligible to register a domain name under .hotel.

.hotel domains will be available for registration to all companies which are member of the Hotel Community on a local, national and international level. The registration of .hotel domain names shall be dedicated to all entities and organizations representing such entities which fulfil the ISO definition quoted above:

1. Individual Hotels
2. Hotel Chains
3. Hotel Marketing organizations representing members from 1. and⁄or 2.
4. International, national and local Associations representing Hotels and Hotel Associations representing members from 1. and⁄or 2.
5. Other Organizations representing Hotels, Hotel Owners and other solely Hotel related organizations representing on members from 1. and⁄or 2.

These categories are a logical alliance of members, with the associations and the marketing organizations maintaining membership lists, directories and registers that can be used, among other public lists, directories and

registers, to verify eligibility against the .hotel Eligility requirements.

The Hotel Community is clearly delineated, well organized, and pre-existing. This can be demonstrated by many Hotel Associations which organize the representation of hotels' interests towards their target groups (businesses, administration and customers). Among those associations the International Hotel and Restaurant Association (IH&RA) is the oldest one, which was founded in 1869⁄1946, is the only global business organization representing the hotel industry worldwide and it is the only global business organization representing the hospitality industry (hotels and restaurants) worldwide. Officially recognized by United Nations as the voice of the private sector globally, IH&RA monitors and lobbies all international agencies on behalf of this industry. Its members represent more than 300,000 hotels and thereby the majority of hotels worldwide.

Among community activities international and national congresses play an important role. In addition, many hotel associations and their members use online communication tools such as newsletter, blogs, Facebook and their own websites to communicate with members, customers and industry partners. The biggest gathering of the global Hotel Community is the annual trade show (Internationale Tourismus Boerse – ITB) in Berlin with over 10,000 exhibitors from 180 countries. Hotel Top-Level-Domain S.a.r.L. participates regularly at national and international congresses, trade shows, is invited speaker and cited in relevant media. The string ".hotel" has no other significant meaning, it only stands for Hotels according to the ISO definition. Including the IH&RA, the majority of the Hotel Community support the initiative by Hotel Top-Level-Domain Sarl, including the definition of the community, the Eligibility Requirements, Content Policy and other related domain policies.

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

HOTEL Top-Level-Domain S.a.r.l. is a member of several hotel associations, e.g.

- International Hotel & Restaurant Association (IH&RA), Lausanne, Switzerland
- American Hotel & Lodging Association (AH&LA), Washington, DC, USA
- Pacific Asia Travel Association (PATA), Bangkok, Thailand
- Deutscher Hotelverband IHA, Berlin, Germany

The Managing Director of HOTEL Top-Level-Domain S.a.r.l., Johannes Lenz-Hawliczek, serves on the Board of Directors of the IH&RA. The board of IH&RA consists of XX members, they represent Hotels, Hotel Chains, …

HOTEL Top-Level-Domain S.a.r.l. is supported by these organizations as well as by

- International Hotel & Restaurant Association (IH&RA), Lausanne, Switzerland,
- American Hotel & Lodging Association (AH&LA), Washington, DC, USA,
- HOTREC (Hospitality Europe), Brussels, Belgium (European Hotel Meta-Association),
- China Hotel Association (CHA), Beijing, China,
- Global Hotel Alliance, Geneva, Switzerland,

and many more including support letters from leading hotel associations from other continents such as from the Argentinian and South African Hotel Association. The support letters are provided in #20f.

* Accountability to the Community *

The Advisory Board of HOTEL Top-Level-Domain S.a.r.l. was set up to advise,

support and make recommendations to the Directors of HOTEL Top-Level-Domain with respect to:

- matters within the areas of their experience and expertise
- the scope of the approval of the .hotel top-level domain
- its subsequent operation.

In addition, the .hotel Advisory Board provides assistance and guidance in

- governing the organization by establishing policies and objectives;
- supporting and reviewing the performance of the management team;
- supporting and reviewing the company's strategy;
- broadening the multi-stakeholder approach and networking of the .hotel top-level domain;
- accounting to the stakeholders for the organization's performance;
- developing domain name registration policies (allocation and administration of domain names).

The members of the .hotel Advisory Board are:

Dr. Ghassan Aidi, President & CEO, International Hotel & Restaurant Association (IH&RA), Lausanne, Switzerland, as a representative of the global hotel association estimated to comprise 300,000 hotels and 8 million restaurants, employ 70 million people and contribute 950 billion USD annually to the global economy.

Markus Luthe, Member of the Executive Committee, Hotels, Restaurants and Cafés in Europe HOTREC, Brussels, Belgium, as representative of a continental hotel organization. HOTREC is the trade association of hotels, restaurants and cafes in the European Union. It is the Voice of Hotels, Restaurants, Cafés and similar establishments in Europe, bringing together 43 national associations representing the hospitality sector - which is composed mainly by SMEs - in 26 countries across Europe, from Portugal to Estonia and from Ireland to Cyprus.

Joe McInerney, President and CEO, American Hotel & Lodging Association (AH&LA), Washington, DC, USA, as representative of a national hotel organization. Serving the hospitality industry for more than a century, AH&LA is the sole national association in the US representing all sectors and stakeholders in the lodging industryI and partnered with 41 state associations to provide local representation.

Nancy Johnson, Executive Vice President, Carlson Hotels Worldwide, Minnetonka, MN, USA, as representative of an International Hotel Chain. Mrs. Johnson is also the current chair (2011⁄2012) of the AH&LA. In her role with Carlson, Johnson oversees business development efforts for Carlson Hotels' select service hotel brands in the Americas including, Country Inns & Suites By Carlson and Park Inn.

Philipp Grabensee, Chairman of the Board, Afilias Ltd, Dublin, Ireland, as representative of the Domain Name Industry. Afilias is a global provider of Internet infrastructure services that connect people to their data. Afilias' reliable, secure, scalable, and globally available technology supports a wide range of applications including Internet domain registry services and Managed DNS.
Accountability

The Accountability mechanisms of the applicant to the Hotel Community include
- A multi-stakeholder staffed Advisory Board that also acts an ombudsman
- A Globally protected Hotel Marks' List as reserved names to protect community interests
- Distribution of annual reports of the HOTEL Top-Level-Domain Sarl about the .hotel top-level domain within the Hotel Community (planned)
- Educational papers, speeches and other public awareness on the .hotel top-level domain (already on-going)

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

* Intended registrants *

Intended registrants of the .hotel domain names are hotels and their organizations worldwide. The .hotel namespace will be exclusive for the Hotel Community. Registrations will be validated for their eligibility according to the .hotel Eligibility criteria:

.hotel domains will be available for registration to all companies which are a member of the Hotel Community on a local, national and international level. The registration of .hotel domain names shall be exclusively limited to the following Hotel Community categories:

1. Individual Hotels
2. Hotel Chains
3. Hotel Marketing organizations representing members from 1. and⁄or 2.
4. International, national and local Associations representing Hotels and Hotel Associations representing members from 1. and⁄or 2.
5. Other Organizations representing Hotels, Hotel Owners and other solely Hotel related organizations representing on members from 1. and⁄or 2.

Each of these Hotel Community members will benefit from a .hotel domain. As presented in response #18, a .hotel domain will increase visibility, be easily discoverable via search engines, provide increased margins through more direct booking options, and have a positive reputation as a namespace to find legitimate hotels.

* Intended Users *

Users of the .hotel domain names will be the members of the global Hotel Community (mainly as suppliers) and all Internet users globally (mainly as consumers and users).

* Related activities *

HOTEL Top-Level-Domain Sarl has carried out global outreach and educational activities within the Hotel Community and its stakeholders at national and international hotel related events such as the
Annual Congresses of the American Hotel & Lodging Association (AH&LA) in New York, since 2010, theAnnual Congresses and Meetings of the International Hotel & Restaurant Association (IH&RA) in Washington, Geneva, Barcelona, Kathmandu, Belgrade, Burgas since 2009, the Annual Congress of the Pacific Asia Travel Association PATA, 2011 in Beijing, the National congresses of German Hotel Association, since 2010, the Meetings of the European Hotel Association HOTREC, since 2011, the Meetings with Hotel Community stakeholders at the world largest tourism fair ITB in Berlin, since 2008.

In conjunction with international press activities, we are maintaining a comprehensive website with articles on .hotel and related topics. In the past, dotHotel has provided extensive guidelines of digital marketing strategies for Hotels; these efforts will continue in the future.

* Lasting nature *

The .hotel top-level domain and its purpose are of a long-lasting nature since digital marketing and distribution and individual digital addresses (domain

names) have become an integral component of a hotel's general business practices and thereby also for the Hotel Community as a whole. It is foreseeable and anticipated that digital strategies including .hotel domain names will play an ever increasing role for hotels within the next decade and beyond. The .hotel top-level domain will thereby serve the Hotel Community and its members in a lasting nature and will fulfil its purpose of providing verified, meaningful and easily recognizable domains.

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

* Relationship "Name and Community" *

The proposed top-level domain name, "HOTEL", is a widely accepted and recognized string that globally identifies the Hotel Community and especially its members, the hotels. Therefore there is a very strong relationship between the applied-for string and the name of the community.

According to the International Standardization Organization, "A hotel is an establishment with services and additional facilities where accommodation and in most cases meals are available." (ISO 18513:2003). Another definition states that "A hotel is an establishment that provides paid lodging on a short-term basis" (Wikipedia). Hotel operations vary in size, function, and cost. Most hotels and major hospitality companies that operate hotels have set widely accepted industry standards to classify hotel types.

* Relationship "Name and Community members" *

The global Hotel Community consists of more than 500,000 hotels and their associations, all being members of the Hotel Community. There is a very strong relationship also between the members of Hotel Community and the applied-for string, as the string "HOTEL" is the word that is uniting them all. Community members can be clearly identified if they fulfil the requirements of ISO 18513:2003.

* Other connotations *

The word hotel has no other significant meaning and is being understood worldwide to mean establishments of the type described above.

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

* Eligibility *

.hotel second-level domain names are initially restricted to the narrow category of hotels and their organizations (Registrants) as defined by ISO 18513. Therefore the registration of .hotel domains shall be exclusively limited to registrants from a logical alliance of the hotel industry including:

1. Individual Hotels
2. Hotel Chains
3. Hotel Marketing organizations representing members from 1. and⁄or 2.
4. International, national and local Associations representing Hotels and Hotel Associations representing members from 1. and⁄or 2.
5. Other Organizations representing Hotels, Hotel Owners and other solely Hotel

related organizations representing on members form 1. and⁄or 2.

It is the role of the .hotel Registry to assure and control the registrant's eligibility to register a domain name to guarantee the community aspect and integrity of the .hotel name space and to avoid disputes. The .hotel Registry anticipates that disputes over the registrant's eligibility will be minimal within the hotel community. Nevertheless it has put in place an adequate procedure to assist the hotel community's registrants in dealing with denials of registrant's eligibility in a way that supports community needs and values. The .hotel Registry's informal denial procedures will not super-cede any formal dispute procedures.

Any domain name registered according to the eligibility criteria described above is subject to a subsequent registrant eligibility verification process which will start immediately after the registration process starts. Registrant eligibility verification will occur after domain name registration but before the registered domain name can be used for web services and protocols like email, website, and FTP. This is to avoid mass fraudulent domain name registrations.

Registrant data supplied for registrant eligibility verification purposes will be held and used by the Registry for eligibility verification purposes only, based on European data protection laws. Registrant eligibility verification requires a review by an applicable organization or by the Registry (reviewer).

The registrant eligibility verification process starts with the Registry evaluation each domain registration for eligibility. For evaluation purposes industry databases will be used, like hotel association databases or other electronically available databases. Within 48 hours after registration started, the registry will provide the evaluation result to the registrar.
In case the reviewer will review the registered domain name and can not validate the domain name he may require further material supporting the registrant's eligibility. Once reviewed the reviewer will confirm or deny the registration. Confirmation will be conveyed to the registrar by email. In the case of denial of the registrant's domain name registration is taken-down in the Registry's discretion. A denial of registrant's eligibility will be recorded against the registrant's domain name and they will not be entitled to register a domain name until their circumstances have changed such that their registrant eligibility is confirmed in the required manner.

Registrant eligibility verification reviews may occur following domain name registration and where a registrant is found to be ineligible subsequent to registration of a domain name(s), and such ineligibility is due to mistake or error on the part of the registrant, their registration fee may be refunded.

The registry confirms registrant's eligibility for up to one year and the registrant may be reviewed annually or at any other time by the Registry to ensure that registrant's eligibility data have not changed in the prior period and that they continue to be eligible. If any change has occurred the registrant at any time may re-submit their registrant's eligibility data and it may be reviewed and confirmed as for initial registrant eligibility verification.

The registrant's eligibility is the central requirement to hold a .hotel domain name. It is therefore necessary that registrants maintain their eligibility throughout the term of the registration, including renewal. If the registrant ceases to be a member of the hotel community as defined by current policies and practices of the Registry, then the registrant must give notice of such change within 20 days of ceasing to be eligible to the registrar.

In the event that the registrant does not notify the Registrar of a change of status, the registrar will report to the registry and the registry may take-down all registrations held by the registrant immediately upon becoming informed of the change of status. The Registry may require further information

from the registrant to determine registrant's eligibility.

In addition to the obligation on the registrant to notify the Registrar of any change of its status, each hotel community that is assisting the Registry in the registrant eligibility verification process may be required to solicit and receive an update of all registrant eligibility verification data from each registrant. Any registrant eligibility verification organization shall provide the Registry with all such information and shall confirm to the Registry that the registrant continues to be eligible to hold the domain name it has registered. In the event that the registrant is no longer entitled to hold the domain name, the Registry shall inform the registrar and the registrar the registrant of that determination and the registrant will be given 20 days to provide updated and correct data that confirms its eligibility. Where such information is not provided, or, if provided, does not support the registrant's eligibility, the Registry will so inform the registrant and provide the registrant with a right to request a review of the denial as if it had been an initial registration. At the time when such review period has ended and the registrant remains ineligible, the Registry shall take-down the domain name and it has to be returned to the list of available domain names.

The Registry's rights to require notice of a change of status, to take-down a domain name unilaterally and to require information is contained in the registrant agreement of the registrar by reference to these policies.

* Types of names *

The Registry will set aside a list of domain names that will be reserved for the 325 major hotel industry brands including sub-brands. Cut-off date for this list is September 2011. These names can be released by the Registry upon request of the brand concerned and registered by eligible community member brand.

* Domain Names available for registration *

No Limitation - Any applicant that is eligible will be entitled to register any domain name that is not reserved or registered at the time of their registration submission through an ICANN accredited registrar.

No Limitation in Number - Registrants are not limited in the number of domain names they may register.

Registrant Representations - The registration application and registrant agreement will contain positive representations from the registrant that they are entitled to the domain name(s) they are or have registered. Breach of such representation will allow the Registry to take-down ineligible domain names at any time.

* Content and Use Restrictions *

The Registry has in its discretion developed restrictions on the content and use of any domain name. Such restrictions apply to any domain name registration that occurs after such restrictions come into effect.

Each domain name must, within one year following the date of registration, and thereafter throughout the term of the domain name registration, be used as the domain name for a website displaying hotel community related content relevant to the domain name, or in such other manner (such as email) that the Registry may approve after review. Domain names used as contemplated above may resolve directly to the relevant website or be forwarded or redirected to another domain name displaying hotel content relevant to the domain name.

Restrictions may include, but are not limited to, a requirement to develop a website that uses the registered domain name, to ensure that each registered domain name resolves to a working website, or to ensure that each website using a registered domain name, or redirected from a registered domain name presents content related to the registered .hotel domain name.

The .hotel Registry will, from time to time in its sole discretion or upon evidence or advice, but at least once a year, conduct continuing or recurring audits of domain names registered to ensure continued compliance with these requirements. Failure to comply will result in a notice providing 20-days to comply. Non-compliance following such a notice period may result in take-down of the relevant domain name, at the discretion of the Registry.

* Enforcement and dispute policy *

The registry will set-up a process for any questions and challenges that may arise from registrations. Complainants will be provided a single point of contact via the registry's website to submit any questions and complaints regarding alleged abuse. The registry will randomly check 2% of registered domains to verify they have content. The registry also follows the standard dispute policies as defined in Q 28 and Q 39.

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.

Hotel Top-Level-Domain S.a.r.l. will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).
Hotel Top-Level-Domain S.a.r.l. will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.
Considering the Governmental Advisory Committee (GAC) advice "Principles

regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs, before the TLD is introduced (Sunrise), so that no parties may apply for them. Hotel Top-Level-Domain S.a.r.l. will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.
Hotel Top-Level-Domain S.a.r.l. will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, Hotel Top-Level-Domain S.a.r.l. will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. Hotel Top-Level-Domain S.a.r.l. will allow the designated beneficiary (the Registrant) to register the name, with an accredited Afilias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.
As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.
If internationalized domains names (IDNs) are introduced in the TLD in the future, Hotel Top-Level-Domain S.a.r.l. will also reserve the IDN versions of the country names in the relevant script(s) before IDNs become available to the public. If we find it advisable and practical, Hotel Top-Level-Domain S.a.r.l. will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.
Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute
Resolution Policy (UDRP), and to any properly-situated court proceeding. Hotel Top-Level-Domain S.a.r.l. will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, Hotel Top-Level-Domain S.a.r.l. will institute a provision to suspend domains names in the event of a dispute. Hotel Top-Level-Domain S.a.r.l. may exercise that right in the case of a dispute over a geographic name.

Registry Services

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

Throughout the technical portion (#23 - #44) of this application, answers are provided directly from Afilias, the back-end provider of registry services for this TLD. HOTEL TOP-LEVEL-DOMAIN S.A.R.L. chose Afilias as its back-end provider because Afilias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afilias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afilias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for this TLD will be performed by Afilias in the same responsible manner used to support 16 top level domains today. Afilias supports more ICANN-contracted TLDs (6) than any other provider currently. Afilias' primary corporate mission is to deliver secure, stable and reliable registry services. This TLD will utilize an existing, proven team and platform for

registry services with:

• A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
• A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
• A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
• Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
• A registry platform that is both IPv6 and DNSSEC enabled;
• An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
• Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
• Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD in accordance with the specific policies and procedures of HOTEL TOP-LEVEL-DOMAIN S.A.R.L. (the "registry operator"), leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

* Registry services to be provided *

To support this TLD, HOTEL TOP-LEVEL-DOMAIN S.A.R.L. and Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:
• Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
• Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias' industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
• Dissemination of TLD zone files: Afilias' distinctive architecture allows for real-time updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
• Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by

reference.
• Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.
• DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

* Security *

Afilias addresses security in every significant aspect – physical, data and network as well as process. Afilias' approach to security permeates every aspect of the registry services provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

* New registry services *

No new registry services are planned for the launch of this TLD.

* Additional services to support registry operation *

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:

• Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
• Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

* Reporting provided to registry operator *

Afilias provides an extensive suite of reports to the registry operator, including daily, weekly and monthly reports with data at the transaction level that enable the registry operator to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. This can be arranged by informing the Afilias Account Manager regarding who should have access. Afilias' data warehouse capability enables drill-down analytics all the way to

the transaction level.

* Reporting available to registrars *

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:
• Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
• Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
• Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

* Financial reporting *

Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit⁄Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

* Afilias approach to registry support *

Afilias, the back end registry services provider for this TLD, is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has worked closely with HOTEL TOP-LEVEL-DOMAIN S.A.R.L. to review specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44, drafted by Afilias given HOTEL TOP-LEVEL-DOMAIN S.A.R.L. requirements. Afilias and HOTEL TOP-LEVEL-DOMAIN S.A.R.L. also worked together to provide financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed

and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afilias is well versed in. Afilias' human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS, or < and >), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

Answers for this question (#24) are provided directly from Afilias, the back-end provider of registry services for this TLD.

Afilias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afilias:

• Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
• Is committed to continuously enhancing our SRS to meet existing and future needs;
• Currently exceeds contractual requirements and will perform in compliance with Specification 10 of the new gTLD Registry Agreement;
• Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of this TLD, and;
• Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afilias registry platform and support the TLD in a secure, stable and reliable manner.

Description of operation of the SRS, including diagrams

Afilias' SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afilias. The Afilias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afilias SRS functionality includes:
• Domain registration: Afilias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.
• Domain renewal: Afilias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
• Transfer: Afilias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
• RGP and restoring deleted domain registrations: Afilias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
• Other grace periods and conformance with ICANN guidelines: Afilias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afilias registry system supports the evolving ICANN guidelines on IDNs.

Afilias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afilias provides "thick" registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afilias' SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD's respective domain policies. With over a decade of experience, Afilias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

* SRS servers and software *

All applications and databases for this TLD will run in a virtual environment

currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the "latest"; the Afilias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS⁄SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:

- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- SAN switches: Brocade 5100
- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through "normal" operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afilias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

* SRS diagram and interconnectivity description *

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a 〈n+1〉 setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afilias SRS technical and operational capabilities (displayed

in Figure 24-a) include:

• Geographically diverse redundant registry systems;
• Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
• Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
• Detailed and tested contingency plan, in case of primary site failure, and;
• Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afilias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

* Synchronization scheme *

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony “sleeps” until a transaction arrives or for one minute, whichever comes first. Slony “wakes up” each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

* SRS SLA performance compliance *
Afilias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afilias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afilias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afilias, on behalf of HOTEL TOP-LEVEL-DOMAIN S.A.R.L. , will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afilias services and infrastructure are designed to scale both vertically and horizontally without any downtime to provide consistent performance as this TLD grows. The Afilias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afilias' experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

* SRS resourcing plans *

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afilias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afilias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afilias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afilias infrastructure, and maintain it. Together, the Afilias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for this TLD.

25. Extensible Provisioning Protocol (EPP)

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS, or < and >), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

Answers for this question (#25) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02⁄00. Afilias has a track record of supporting TLDs on standards-compliant versions of EPP. Afilias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afilias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afilias' EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:

• A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD's needs;
• A track record of success in developing extensions to meet client and registrar business requirements such as multi-script support for IDNs;
• Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
• EPP software that is operating today and has been fully tested to be standards-compliant;
• Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
• An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afilias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

* EPP Standards *

The Afilias registry system complies with the following revised versions of the RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance ("QA") team for RFC compliance, and have been used by registrars for an extended period of time:

• 3735 - Guidelines for Extending EPP
• 3915 - Domain Registry Grace Period Mapping
• 5730 - Extensible Provisioning Protocol (EPP)
• 5731 - Domain Name Mapping
• 5732 - Host Mapping
• 5733 - Contact Mapping
• 5734 - Transport Over TCP
• 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afilias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afilias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afilias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afilias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

* EPP software interface and functionality *

Afilias will provide all registrars with a free open-source EPP toolkit. Afilias provides this software for use with both Microsoft Windows and Unix⁄Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator's website.

Afilias' SRS EPP software complies with all relevant RFCs and includes the following functionality:

• EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the

text response supported, and one or more elements which identify the objects that the server is capable of managing;
• Session management controls: 〈login〉 to establish a connection with a server, and 〈logout〉 to end a session;
• EPP Objects: Domain, Host and Contact for respective mapping functions;
• EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
• EPP Object Transform Commands: five commands to transform objects: 〈create〉 to create an instance of an object, 〈delete〉 to remove an instance of an object, 〈renew〉 to extend the validity period of an object, 〈update〉 to change information associated with an object, and 〈transfer〉 to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afilias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afilias SRS registry. Afilias' EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

*Free EPP software support *

Afilias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires mutual authentication; Afilias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afilias will provide free guidance for registrars unfamiliar with this requirement.

*Registrar data synchronization *

There are two methods available for registrars to synchronize their data with the registry:
• Automated synchronization: Registrars can, at any time, use the EPP 〈info〉 command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.

• Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

* EPP modifications *

There are no unique EPP modifications planned for this TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:

• An 〈ipr:name〉 element that indicates the name of Registered Mark.
• An 〈ipr:number〉 element that indicates the registration number of the IPR.
• An 〈ipr:ccLocality〉 element that indicates the origin for which the IPR is established (a national or international trademark registry).
• An 〈ipr:entitlement〉 element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
• An 〈ipr:appDate〉 element that indicates the date the Registered Mark was applied for.

• An 〈ipr:regDate〉 element that indicates the date the Registered Mark was issued and registered.
• An 〈ipr:class〉 element that indicates the class of the registered mark.
• An 〈ipr:type〉 element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

* EPP resourcing plans *

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

108 Afilias team members directly contribute to the management and development of the EPP based registry systems. As previously noted, Afilias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing needs and forecast registry⁄registrar needs to ensure the Afilias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afilias include: Technical Analysts, the Network Operations Center and Data Services team members.

26. Whois

Answers for this question (#26) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afilias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afilias meets and exceeds ICANN's requirements. Specifically, Afilias will:

• Offer a WHOIS service made available on port 43 that is flexible and standards- compliant;
• Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
• Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
• Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afilias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has

been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afilias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

* WHOIS system description and diagram *

The Afilias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afilias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afilias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

* Data objects, interfaces, access and lookups *

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afilias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:

-The name of the domain registered and the sponsoring registrar;
-The names of the primary and secondary nameserver(s) for the registered domain name;
-The creation date, registration status and expiration date of the registration;
-The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
-The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
-The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
-The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.
The following additional features are also present in Afilias' WHOIS service:
-Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
-Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

* Query controls *

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If

object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:

-Domain: Searches only domain objects. The input string is searched in the Name field.
-Host: Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
-Contact: Searches only contact objects. The input string is searched in the ID field.
-Registrar: Searches only registrar objects. The input string is searched in the Name field.

By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

* Unique TLD requirements *

There are no unique WHOIS requirements for this TLD.

* Sunrise WHOIS processes *

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:

-Trademark Name: element that indicates the name of the Registered Mark.
-Trademark Number: element that indicates the registration number of the IPR.

-Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
-Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
- Trademark Application Date: element that indicates the date the Registered Mark was applied for.
-Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
-Trademark Class: element that indicates the class of the Registered Mark.
-IPR Type: element that indicates the Sunrise phase the application applies for.

* IT and infrastructure resources *

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches.
The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:
-Servers: Cisco UCS B230 blade servers
-SAN storage arrays: IBM Storwize V7000 with Solid State Drives
-Firewalls: Cisco ASA 5585-X
-Load balancers: F5 Big-IP 6900
-Traffic shapers: Procera PacketLogic PL8720
-Routers: Juniper MX40 3D
-Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

* Frequency of synchronization between servers *

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

* Specifications 4 and 10 compliance *

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

* RFC 3912 compliance *

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a "thick" registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator's needs.

* Searchable WHOIS *

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afilias WHOIS systems. For instance, Afilias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afilias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afilias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as "Do not redistribute" or "Special access granted". This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afilias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver's IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afilias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see "Query Controls" above for details about search options and capabilities.

* Deterring WHOIS abuse *

Afilias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. The registry operator will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit(/48) prefix. If another offending IPv6 address does fall into the /48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (/48) network. As a security precaution, Afilias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee's deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

* WHOIS staff resourcing plans *

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

27. Registration Life Cycle

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS, or 〈 and 〉), WHICH ICANN INFORMS US (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER BELOW AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED. THEREFORE, THE FULL ANSWER TO THIS QUESTION IS ALSO ATTACHED AS A PDF FILE, ACCORDING TO SPECIFIC GUIDANCE FROM ICANN UNDER CASE ID 11027.

Answers for this question (#27) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias has been managing registrations for over a decade. Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program[s], Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5.

* Registration period *

After the IP protection programs and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol ("EPP") commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:
• The domain must be unique;

• Restricted or reserved domains cannot be registered;
• The domain can be registered from 1-10 years;
• The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
• The domain can be explicitly deleted at any time;
• The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a transfer; and,

Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.
• OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
• Inactive: The domain has no delegated name servers.
• Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be

associated to, or disassociated from the domain. This status includes: Delete Prohibited ⁄ Server Delete Prohibited, Update Prohibited ⁄ Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
• Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.
• Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.
a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:
i. Registrant Contact
ii. Admin Contact
iii. Technical Contact
iv. Billing Contact
v. Host or nameservers
vi. Authorization information
vii. Associated status values
A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.
b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:
i. A domain can be renewed at any time during its registration term,
ii. The registration term cannot exceed a total of 10 years.
A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.
c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:
i. A domain can be deleted at any time during its registration term, f the domain is deleted during the Add Grace Period or the Renew⁄Extend Grace Period, the sponsoring registrar will receive a credit,
ii. A domain cannot be deleted if it has “child” nameservers that are associated to other domains.
A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.
d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.
i. The registrant must obtain the applicable 〈authInfo〉 code from the sponsoring (losing) registrar.
• Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the "password" to the domain).
• Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.
ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the authInfo code.
• Every EPP 〈transfer〉 command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.
iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.
• When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.
• If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be

required to reinitiate the process.
• If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.
iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.
v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.
vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.
vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.
e. Bulk transfer: Afilias, supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.

HOTEL TOP-LEVEL-DOMAIN S.A.R.L. will support ICANN's Transfer Dispute Resolution Process. HOTEL TOP-LEVEL-DOMAIN S.A.R.L. will work with Afilias to respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

1. Auto-renew grace period

The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:
i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

2. Redemption grace period

During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

3. Pending delete

During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

* Other grace periods *

All ICANN required grace periods will be implemented in the registry backend service provider's system including the Add Grace Period (AGP), Renew/Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period (RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

* Add grace period *

The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew/Extend, or Transfer operation occurs within the five calendar days, the following rules apply.
i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the registry backend service provider's database and is released back into the pool of available domains.
ii. Renew/Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.
iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

* Renew / extend grace period *

The Renew / Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:
i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew/Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.
If a domain is auto-renewed, then extended, and then deleted within the Renew/Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were

added to the domain's expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

* Transfer Grace Period *

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew/Extend occurs within that five calendar days, the following rules apply:
i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the renewal years as long as the total term does not exceed 10 years.

This TLD will conduct an auction for certain domain names. Afilias will manage the domain name auction using existing technology. Upon the completion of the auction, any domain name acquired will then follow the standard lifecycle of a domain.

* Registration lifecycle resources *

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afilias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:
a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the existing gTLDs.
b. Afilias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs change.

Afilias has more than 30 staff members in these departments.

28. Abuse Prevention and Mitigation

HOTEL TOP-LEVEL-DOMAIN S.A.R.L., working with Afilias, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to:
• Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;

• Committing to rapid identification and resolution of abuse, including suspensions;
• Ensuring completeness of WHOIS information at the time of registration;
• Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
• Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

Abuse policy
The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name 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. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti -abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

.hotel Anti-Abuse Policy
The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:
• Illegal or fraudulent actions;
• Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
• Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
• Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
• Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
• Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
• Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
• Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking").

Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (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 registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

Abuse point of contact and procedures for handling abuse complaints
The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.hotel". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
• Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
• The identity of a proxy-protected registrant;
• The purchaser's IP address;
• Whether there is a reseller involved, and;
• The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected 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; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority

and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
• Registration information
• History of a domain, including recent updates made
• Other domains associated with a registrant's account
• Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
• Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
• Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
• Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:
• Number of abuse reports received by the registry's abuse point of contact described above;
• Number of cases and domains referred to registrars for resolution;
• Number of cases and domains where the registry took direct action;
• Resolution times;
• Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;
• Phishing site uptimes in the TLD.

Removal of orphan glue records
By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: http://www.icann.org/en/committees/security/sac048.pdf.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. 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. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check 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 the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records

that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by nameserver report" to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

Methods to promote WHOIS accuracy
The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

WHOIS data accuracy
The registry operator 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 better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide

to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars
As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar⁄Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http:⁄⁄wdprs.internic.net⁄).

Controls to ensure proper access to domain functions
Several measures are in place in the Afilias registry system 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, TLS⁄SSL certificates and proper authentication are used to control access to the registry system. Registrars are only given access to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code. 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 in order 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.

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

Validation and abuse mitigation mechanisms
Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

Registrant pre-verification and authentication
One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to

billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

• Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
• Based on required WHOIS Data; registrant contact details (name, address, phone)
• If address⁄ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
• If in-line processing and registration and EPP⁄API call would go to the verification clearinghouse and return up to 4 challenge questions.
• If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
• If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
• WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a “privacy service”.
• A “Validation Icon” customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would should limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
• Validation would be annually renewed, and validation date displayed in the WHOIS.

Abuse prevention resourcing plans
Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias’ 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

This TLD’s anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias and the registry operator’s anti-abuse function anticipates the expected volume and type of registrations, and

together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally a security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:
• Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry’s eligibility restrictions or policies);
• Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse,

the services of one of ICANN's approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
• Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
• Complying with the URS requirements;
• Complying with the UDRP;
• Complying with the PDDRP, and;
• Including all ICANN-mandated and independently developed rights protection mechanisms ("RPMs") in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD
The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

* Sunrise period *

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the TLD. Following the Sunrise Period, HOTEL TOP-LEVEL-DOMAIN S.A.R.L. will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:

• Launch of the TLD – Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in the TLD. To maximize fairness registrations will be processed via a randomized, round robin system, which will close 60 days following the Sunrise launch date respectively. Following this, HOTEL TOP-LEVEL-DOMAIN S.A.R.L. expects the balance of Sunrise registrations to be awarded in real-time.
• Two months after launch –The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.
• One month after close of Quiet Period – Registration in the TLD domain will be opened to qualified applicants.
• Immediately after launch the TLD's domain names begin to resolve through standard Web browsers.

* Sunrise Period Requirements & Restrictions *

Those wishing to reserve their marks in the TLD during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term of five years.

HOTEL TOP-LEVEL-DOMAIN S.A.R.L. will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP).

The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants 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.

* Ongoing rights protection mechanisms *

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

* Uniform Rapid Suspension (URS) *

The registry operator will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN’s Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator’s support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN’s URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall “lock” the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will “lock” the domain by associating the following EPP statuses with the domain and relevant contact objects:

• ServerUpdateProhibited, with an EPP reason code of “URS”
• ServerDeleteProhibited, with an EPP reason code of “URS”
• ServerTransferProhibited, with an EPP reason code of “URS”
• The registry operator’s support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator’s support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator’s support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the "registry operator 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."

* Rights protection via the RRA *

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

• The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
a. to enforce registry policies and ICANN requirements; each as amended from time to time;
b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
c. to protect the integrity and stability of the registry, its operations, and the TLD system;
d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

* Reducing opportunities for behaviors such as phishing or pharming *

In our response to question #28, the registry operator has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

With specific respect to phishing and pharming, it should be noted by ICANN that this will be a single entity TLD in which HOTEL TOP-LEVEL-DOMAIN S.A.R.L. has direct control over each registrant (they are typically on staff or otherwise contractually bound) and how each registration may be used. Further, there will be no open registration period for this TLD, as it will never be an "open" TLD. Since all criminal activity (such as phishing and pharming) is precluded by the mission, values and policies of the registry operator (and its parent organization), criminal activity is not expected to be a problem. If such activity occurs due to hacking or other compromises, the registry operator will take prompt and effective steps to eliminate the activity.

In the case of this TLD, HOTEL TOP-LEVEL-DOMAIN S.A.R.L. will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows HOTEL TOP-LEVEL-DOMAIN S.A.R.L. internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

* Rights protection resourcing plans *

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias and the support staff of the registry operator, which is on duty 24x7. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

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

The answer to question #30a is provided by Afilias, the back-end provider of registry services for this TLD.

Afilias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afilias' robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afilias will continue these rigorous security measures, which include:
• Multiple layers of security and access controls throughout registry and support systems;
• 24x7 monitoring of all registry and DNS systems, support systems and facilities;
• Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
• Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
• Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

* Security policies and protocols *

Afilias has included security in every element of its service, including facilities, hardware, equipment, connectivity⁄Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow⁄insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our

response to question #30(b).

There are several important aspects of the security policies and procedures to note:
• Afilias hosts domains in data centers around the world that meet or exceed global best practices.
• Afilias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
• Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
• Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
• All registry components – critical and non-critical – are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afilias follows the guidelines from the ISO 27001 Information Security Standard (Reference: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) for the management and implementation of its Information Security Management System. Afilias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: http://www.isaca.org/cobit). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afilias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: http://www.itil-officialsite.com/).

The Afilias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afilias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afilias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

* Access to registry system *

Access to all production systems and software is strictly limited to authorized

operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

Afilias applications use encrypted network communications. Access to the registry server is controlled. Afilias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry's own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both certificate checks and login/password combinations. Web connections are encrypted using TLS/SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login/password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.

To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afilias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

* Independent assessment *

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:
• Access control;
• Security policies;
• Production change control;
• Backups and restores;
• Batch monitoring;
• Intrusion detection, and
• Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in

place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:

• Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
• Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
• Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
• Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
• Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

* Special TLD considerations *

Afilias' rigorous security practices are regularly reviewed; if there is a need

to alter or augment procedures for this TLD, they will be done so in a planned and deliberate manner.

* Commitments to registrant protection *

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a "thick" registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN's SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:
• Any confidential information stored within the registry will remain confidential;
• The interaction between their registrar and Afilias is secure;
• The Afilias DNS system will be reliable and accessible from any location;
• The registry system will abide by all polices, including those that address registrant data;
• Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped improve registrants' ability to protect their domains name(s) during the domain name lifecycle.
• [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
• [SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
• [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
• [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
• [SAC024]: Report on Domain Name Front Running (February 2008)
• [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
• [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
• [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
• [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS⁄SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24⁄7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised – for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-

through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

* Security resourcing plans *

Please refer to our response to question #30b for security resourcing plans.

crowell moring

Annex 8.

New gTLD Program
Community Priority Evaluation Report
Report Date: 11 June 2014

Application ID:	1-1032-95136
Applied-for String:	HOTEL
Applicant Name:	HOTEL Top-Level-Domain s.a.r.l

Overall Community Priority Evaluation Summary

Community Priority Evaluation Result	**Prevailed**

Thank you for your participation in the New gTLD Program. After careful consideration and extensive review of the information provided in your application, including documents of support, the Community Priority Evaluation panel determined that the application met the requirements specified in the Applicant Guidebook. Your application prevailed in Community Priority Evaluation.

Panel Summary

Overall Scoring — 15 Point(s)

Criteria	Earned	Achievable
#1: Community Establishment	4	4
#2: Nexus between Proposed String and Community	3	4
#3: Registration Policies	4	4
#4: Community Endorsement	4	4
Total	15	16

Minimum Required Total Score to Pass 14

Criterion #1: Community Establishment — 4/4 Point(s)

1-A Delineation — *2/2 Point(s)*

The Community Priority Evaluation panel determined that the community as identified in the application met the criterion for Delineation as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the community is clearly delineated, organized and pre-existing. The application received the maximum score of 2 points under criterion 1-A: Delineation.

Delineation
Two conditions must be met to fulfill the requirements for delineation: there must be a clear, straightforward membership definition, and there must be awareness and recognition of a community (as defined by the applicant) among its members.

The community defined in the application ("HOTEL") is:

> The .hotel namespace will exclusively serve the global Hotel Community. The string "Hotel" is an internationally agreed word that has a clear definition of its meaning: According to DIN EN ISO 18513:2003, "A hotel is an establishment with services and additional facilities where accommodation and in most cases meals are available." Therefore only entities which fulfil this definition are members of the Hotel Community and eligible to register a domain name under .hotel. .hotel domains will be available for registration to all companies which are member of the Hotel Community on a local, national and international level. The registration of .hotel domain names shall be dedicated to all entities and organizations representing such entities which fulfil the ISO definition quoted above:
> 1. Individual Hotels
> 2. Hotel Chains
> 3. Hotel Marketing organizations representing members from 1. and/or 2.
> 4. International, national and local Associations representing Hotels and Hotel Associations representing members from 1. and/or 2.
> 5. Other Organizations representing Hotels, Hotel Owners and other solely Hotel related organizations representing on members from 1. and/or 2.
> These categories are a logical alliance of members, with the associations and the marketing organizations maintaining membership lists, directories and registers that can be used, among other public lists, directories and registers, to verify eligibility against the .hotel Eligility requirements.

This community definition shows a clear and straightforward membership. The community is clearly defined because membership requires entities/associations to fulfill the ISO criterion for what constitutes a hotel. Furthermore, association with the hotel sector can be verified through membership lists, directories and registers.

In addition, the community as defined in the application has awareness and recognition among its members. This is because the community is defined in terms of its association with the hotel industry and the provision of specific hotel services.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both the conditions to fulfill the requirements for Delineation.

Organization

Two conditions need to be met to fulfill the requirements for organization: there must be at least one entity mainly dedicated to the community, and there must be documented evidence of community activities.

The community as defined in the application has at least one entity mainly dedicated to the community. There are, in fact, several entities that are mainly dedicated to the community, such as the International Hotel and Restaurant Association (IH&RA), Hospitality Europe (HOTREC), the American Hotel & Lodging Association (AH&LA) and China Hotel Association (CHA), among others. According to the application,

> Among those associations the International Hotel and Restaurant Association (IH&RA) is the oldest one, which was founded in 1869/1946, is the only global business organization representing the hotel industry worldwide and it is the only global business organization representing the hospitality industry (hotels and restaurants) worldwide. Officially recognized by United Nations as the voice of the private sector globally, IH&RA monitors and lobbies all international agencies on behalf of this industry. Its members represent more than 300,000 hotels and thereby the majority of hotels worldwide.

The community as defined in the application has documented evidence of community activities. This is confirmed by detailed information on IH&RA's website, as well as information on other hotel association websites.

The Community Priority Evaluation panel determined that the community as defined in the application

satisfies both the conditions to fulfill the requirements for Organization.

Pre-existence
To fulfill the requirements for pre-existence, the community must have been active prior to September 2007 (when the new gTLD policy recommendations were completed).

The community as defined in the application was active prior to September 2007. Hotels have existed in their current form since the 19th century, and the oldest hotel association is IH&RA, which, according to the entity's website, was first established in 1869 as the All Hotelmen Alliance. The organization has been operating under its present name since 1997.

The Community Priority Evaluation panel determined that the community as defined in the application fulfills the requirements for Pre-existence.

1-B Extension	*2/2 Point(s)*

The Community Priority Evaluation panel determined that the community as identified in the application met the criterion for Extension specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application demonstrates considerable size and longevity for the community. The application received a maximum score of 2 points under criterion 1-B: Extension.

Size
Two conditions must be met to fulfill the requirements for size: the community must be of considerable size and must display an awareness and recognition of a community among its members.

The community as defined in the application is of a considerable size. The community for .HOTEL as defined in the application is large in terms of the number of members. According to the applicant, "the global Hotel Community consists of more than 500,000 hotels and their associations".

In addition, the community as defined in the application has awareness and recognition among its members because the community is defined in terms of association with the provision of hotel services.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both the conditions to fulfill the requirements for Size.

Longevity
Two conditions must be met to fulfill the requirements for longevity: the community must demonstrate longevity and must display an awareness and recognition of a community among its members.

The community as defined in the application demonstrates longevity. The pursuits of the .HOTEL community are of a lasting, non-transient nature.

In addition, the community as defined in the application has awareness and recognition among its members because the community is defined in terms of association with the provision of hotel services.

The Community Priority Evaluation panel determined that the community as defined in the application satisfies both the conditions to fulfill the requirements for Longevity.

Criterion #2: Nexus between Proposed String and Community	**3/4 Point(s)**
2-A Nexus	*2/3 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Nexus as

specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook. The string identifies the name of the community, without over-reaching substantially beyond the community. The application received a score of 2 out of 3 points under criterion 2-A: Nexus.

To receive the maximum score for Nexus, the applied-for string must match the name of the community or be a well-known short-form or abbreviation of the community name. To receive a partial score for Nexus, the applied-for string must identify the community. "Identify" means that the applied-for string should closely describe the community or the community members, without over-reaching substantially beyond the community.

The applied-for string (.HOTEL) identifies the name of the community. According to the applicant,

> The proposed top-level domain name, "HOTEL", is a widely accepted and recognized string that globally identifies the Hotel Community and especially its members, the hotels.

The string nexus closely describes the community, without overreaching substantially beyond the community. The string identifies the name of the core community members (i.e. hotels and associations representing hotels). However, the community also includes some entities that are related to hotels, such as hotel marketing associations that represent hotels and hotel chains and which may not be automatically associated with the gTLD. However, these entities are considered to comprise only a small part of the community. Therefore, the string identifies the community, but does not over-reach substantially beyond the community, as the general public will generally associate the string with the community as defined by the applicant.

The Community Priority Evaluation panel determined that the applied-for string identifies the name of the community as defined in the application. It therefore partially meets the requirements for Nexus.

2-B Uniqueness	*1 / 1 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Uniqueness as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the string has no other significant meaning beyond identifying the community described in the application. The application received a maximum score of 1 point under criterion 2-B: Uniqueness.

To fulfill the requirements for Uniqueness, the string .HOTEL must have no other significant meaning beyond identifying the community described in the application. The Community Priority Evaluation panel determined that the applied-for string satisfies the condition to fulfill the requirements for Uniqueness.

Criterion #3: Registration Policies	**4/4 Point(s)**
3-A Eligibility	*1 / 1 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Eligibility, as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as eligibility is restricted to community members. The application received a maximum score of 1 point under criterion 3-A: Eligibility.

To fulfill the requirements for Eligibility, the registration policies must restrict the eligibility of prospective registrants to community members. The application demonstrates adherence to this requirement by restricting eligibility to the narrow category of hotels and their organizations as defined by ISO 18513, and verifying this association through membership lists, directories and registries. (Comprehensive details are provided in Section 20e of the applicant documentation). The Community Priority Evaluation panel determined that the application satisfies the condition to fulfill the requirements for Eligibility.

3-B Name Selection *1/1 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Name Selection as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as name selection rules are consistent with the articulated community-based purpose of the applied-for gTLD. The application received a maximum score of 1 point under criterion 3-B: Name Selection.

To fulfill the requirements for Name Selection, the registration policies for name selection for registrants must be consistent with the articulated community-based purpose of the applied-for gTLD. The application demonstrates adherence to this requirement by specifying that eligible applicants will be entitled to register any domain name that is not reserved or registered at the time of their registration submission. Furthermore, the registry has set aside a list of domain names that will be reserved for the major hotel industry brands and sub-brands. (Comprehensive details are provided in Section 20e of the applicant documentation). The Community Priority Evaluation panel determined that the application satisfies the condition to fulfill the requirements for Name Selection.

3-C Content and Use *1/1 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Content and Use as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the rules for content and use are consistent with the articulated community-based purpose of the applied-for TLD. The application received a maximum score of 1 point under criterion 3-C: Content and Use.
To fulfill the requirements for Content and Use, the registration policies must include rules for content and use for registrants that are consistent with the articulated community-based purpose of the applied-for gTLD. The application demonstrates adherence to this requirement by specifying that each domain name must display hotel community-related content relevant to the domain name, etc. (Comprehensive details are provided in Section 20e of the applicant documentation). The Community Priority Evaluation panel determined that the application satisfies the condition to fulfill the requirements for Content and Use.

3-D Enforcement *1/1 Point(s)*

The Community Priority Evaluation panel determined that the application met the criterion for Enforcement as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application provided specific enforcement measures as well as appropriate appeal mechanisms. The application received a maximum score of 1 point under criterion 3-D: Enforcement.

Two conditions must be met to fulfill the requirements for Enforcement: the registration policies must include specific enforcement measures constituting a coherent set, and there must be appropriate appeals mechanisms. The applicant outlined policies that include specific enforcement measures constituting a coherent set. The applicant's registry will establish a process for questions and challenges that could arise from registrations and will conduct random checks on registered domains. There is also an appeals mechanism, whereby a registrant has the right to request a review of a decision to revoke its right to hold a domain name. (Comprehensive details are provided in Section 20e of the applicant documentation). The Community Priority Evaluation panel determined that the application satisfies both conditions to fulfill the requirements for Enforcement.

Criterion #4: Community Endorsement **4/4 Point(s)**

4-A Support *2/2 Point(s)*

The Community Priority Evaluation panel determined that the application fully met the criterion for Support

specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the applicant had documented support from the recognized community institution(s)/member organization(s). The application received a maximum score of 2 points under criterion 4-A: Support.

To receive the maximum score for Support, the applicant is, or has documented support from, the recognized community institution(s)/member organization(s), or has otherwise documented authority to represent the community. "Recognized" means the institution(s)/organization(s) that, through membership or otherwise, are clearly recognized by the community members as representative of the community. To receive a partial score for Support, the applicant must have documented support from at least one group with relevance. "Relevance" refers to the communities explicitly and implicitly addressed.

The Community Priority Evaluation panel determined that the applicant was not the recognized community institution(s)/member organization(s). However, the applicant possesses documented support from the recognized community institution(s)/member organization(s), and this documentation contained a description of the process and rationale used in arriving at the expression of support. These groups constitute the recognized institutions to represent the community, and represent a majority of the overall community as defined by the applicant. The Community Priority Evaluation Panel determined that the applicant fully satisfies the requirements for Support.

4-B Opposition ***2 / 2 Point(s)***

The Community Priority Evaluation panel determined that the application met the criterion for Opposition specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the application did not receive any relevant opposition. The application received the maximum score of 2 points under criterion 4-B: Opposition.

To receive the maximum score for Opposition, the application must not have received any opposition of relevance. To receive a partial score for Opposition, the application must have received relevant opposition from, at most, one group of non-negligible size. According to the Applicant Guidebook, "To be taken into account as relevant opposition, such objections or comments must be of a reasoned nature. Sources of opposition that are clearly spurious, unsubstantiated, made for a purpose incompatible with competition objectives, or filed for the purpose of obstruction will not be considered relevant". "Relevance" and "relevant" refers to the communities explicitly and implicitly addressed.

The application received letters of opposition, which were determined not to be relevant, as they were either from groups of negligible size, or were from entities/communities that do not have an association with the applied for string. The Community Priority Evaluation Panel determined that these letters therefore were not relevant because they are not from the recognized community institutions/member organizations, nor were they from communities/entities that have an association with the hotel community. In addition, some letters were filed for the purpose of obstruction, and were therefore not considered relevant. The Community Priority Evaluation Panel determined that the applicant satisfies the requirements for Opposition.

Disclaimer: Please note that these Community Priority Evaluation results do not necessarily determine the final result of the application. In limited cases the results might be subject to change. These results do not constitute a waiver or amendment of any provision of the Applicant Guidebook or the Registry Agreement. For updated application status and complete details on the program, please refer to the Applicant Guidebook and the ICANN New gTLDs microsite at <newgtlds.icann.org>.

crowell moring

Annex 9.

Reconsideration Request Form

Version of 11 April 2013

ICANN's Board Governance Committee is responsible for receiving requests for reconsideration from any person or entity that has been materially affected by any ICANN staff action or inaction if such affected person or entity believes the action contradicts established ICANN policies, or by actions or inactions of the Board that such affected person or entity believes has been taken without consideration of material information. Note: This is a brief summary of the relevant Bylaws provisions. For more information about ICANN's reconsideration process, please visit http://www.icann.org/en/general/bylaws.htm#IV and http://www.icann.org/en/committees/board-governance/.

This form is provided to assist a requester in submitting a Reconsideration Request, and identifies all required information needed for a complete Reconsideration Request. This template includes terms and conditions that shall be signed prior to submission of the Reconsideration Request.

Requesters may submit all facts necessary to demonstrate why the action/inaction should be reconsidered. However, argument shall be limited to 25 pages, double-spaced and in 12 point font.

For all fields in this template calling for a narrative discussion, the text field will wrap and will not be limited.

Please submit completed form to reconsideration@icann.org.

1. Requester Information

1. Name: Despegar Online SRL,

Address: Contact Information Redacted

Contact Information Redacted

Email: Contact Information Redacted

AND

2. **Name:** DotHotel Inc.,

Address: Contact Information Redacted

Contact Information Redacted

Email: Contact Information Redacted

AND

3 **Name:** dot Hotel Limited,

Address: Contact Information Redacted

Email: Contact Information Redacted

AND

4. **Name:** Fegistry, LLC,

Address: Contact Information Redacted

Email: Contact Information Redacted

AND

5. **Name:** Spring McCook, LLC,

Address: Contact Information Redacted

Email: Contact Information Redacted

AND

6. **Name:** Top Level Domain Holdings Limited,

Address: Contact Information Redacted

Email: Contact Information Redacted

(Requester, herein)

(Note: ICANN will post the Requester's name on the Reconsideration Request page at http://www.icann.org/en/committees/board-governance/requests-for-reconsideration-en.htm. Requestors address, email and phone number will be removed from the posting.)

2. Request for Reconsideration of (check one only):

___ Board action/inaction

_X__ Staff action/inaction

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

Requester was notified by public posting at http://newgtlds.icann.org/en/applicants/cpe#invitations on or about 12 June 2014 that the application for the new gTLD .hotel (1-1032-95136) by HOTEL Top-Level-Domain s.a.r.l had prevailed in an award of community priority after Community Priority Evaluation. Requester seeks to have that decision by the Community Priority Evaluation panel reconsidered.

4. Date of action/inaction:

The date of the CPE panel is 11 June 2014; the date of its public posting is approximately 12 June 2014.

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

Requester became aware of the action on or about 13 June 2014

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

Requester is a group of applicants in a contention set with other applicants for .hotel. If the decision to award community priority to application 1-1032-95136 stands, it will require Requesters' standard (non-community) applications to be abandoned or withdrawn. The Applicant Guidebook ("AGB") states at page 4-9:

"It should be noted that a qualified community application eliminates all directly contending standard applications, regardless of how well qualified the latter may be."

"Qualified" in this context means that the application has been awarded community priority status. The elimination of Requester's applications will cause Requester to lose its current investment of

time, money and other resources in its applications, notwithstanding the availability of a small application fee refund. More significantly, it deprives Requester of the opportunity to run the .Hotel TLD, which represent loss of a financial and business opportunity to Requestor.

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

The purpose behind the community application is expressly to fend off legitimate competition from business operators in competition with the standard hotel booking model. Community applicants are required to file evidence of support from their so-called community. This applicant has filed support from commercial trade associations dependent on maintaining the current commercial model.

The Applicant's principal supporter is the IH&RA (International Hotel and Restaurant Association).

The IH &RA said, in its supporting letter:

We fully support dotHOTEL's Eligibility Criteria as defined in ISO 18513 to establish a verified and secure domain name space exclusively for the hotel industry. Thus, .hotel domain names will help to increase direct bookings by which profit margins of hotels rise and to reduce dependency from OTAs.

The Hotrec association (a trade association supporting both the restaurant and hotel trades in Europe) said this:

"... hotels all over Europe are concerned to lose more and more control over their rates, distribution channels and the hotel product itself to the so-called Online Travel Agencies or OTAs. With dotHOTEL's Eligibility Criteria for a verified and secure domain name space exclusively for the hotel industry as defined in ISO 18513, .hotel domain names will help to increase direct bookings by which profit margins of hotels rise and to reduce dependency from OTAs."

The Global Hotel Alliance said:
"....hotels all over the union are concerned to lose more and more control over their rates, distribution channels and the hotel product itself to the so called Other Travel Agencies or OTAs. With dotHotel's eligibility criteria for a verified and secure domain name space exclusively for the hotel industry as defined in ISO 18513 .hotel domain names will help to increase direct bookings by which profit margins of hotels rise and to reduce dependency on OTAs."

The application is plainly a purely commercial move by heavily invested commercial entities to increase their profits, and to head off competition from developing threats to their market, presented by the growth of the OTA business model.

Other parties affected by the decision therefor include all of the world's OTAs, and all of the

world's customers of hotel products that will be deprived of competitive business opportunities in relation to hotel bookings.

8. Detail of Board or Staff Action – Required Information

Introduction

Requester submits that the Community Priority Evaluation Panel ("Panel") failed to properly perform its functions as set out in the AGB.

Before describing the failures of the Panel, Requester makes two procedural comments.

First, there is no doubt that ICANN's Reconsideration process applies to the decisions of external providers such as the Panel. As noted by the Board Governance Committee ("BGC") in the recent .tennis decision:

"ICANN has previously determined that the reconsideration process can properly be invoked for challenges to expert determinations rendered by panels formed by third party service providers, such as the EIU, where it can be stated that the Panel failed to follow established policies or processes in reaching its determination, or that staff failed to follow its policies or processes in accepting that determination."[1]

Second, the Requester appreciates that on Reconsideration by the BGC, the Requester bears the burden of proving that the Panel has failed to follow some policy or process that it should have done, and is not a challenge to the accuracy or validity of any of the Panel's conclusions. The Requester apprehends the BGC position that disagreeing with the conclusion of the Panel is not sufficient grounds for reconsideration. As the BGC noted in the .tennis Decision on reconsideration:

"In challenging the Panel's Report, the Requester does not identify any process or policy or standard that the Panel misapplied in scoring element 2-A. Instead, the Requester simply objects to the Panel's substantive conclusion, arguing that "[t]he community as defined [in the Application] specifically includes the global tennis community." (Request at 4.) Such substantive disagreement with the Panel's findings is not a proper basis for reconsideration."
[2]

In this case, however, there are 3 instances where the Panel has not followed the AGB policy and processes for conducting CPE.

Further, the Panel, and ICANN staff have breached more general ICANN policies and procedures in the conduct of this CPE.

Breaches of the AGB rules on Community Priority Evaluation.

---

[1] *See* http://www.icann.org/en/groups/board/governance/reconsideration/recommendation-booking-01aug13- en.doc, BGC Recommendation on Reconsideration Request 13-5.

[2] https://www.icann.org/en/system/files/files/determination-tennis-au-29apr14-en.pdf

1. Failure to identify a "Community".

The AGB sets out at para 4.2.3 the rules for community priority. In doing so, the drafting practice has been to set out a rule, in this criteria for awarding points, then to provide definitions of the terms used in the criteria, and then guidelines on how to apply the definitions and interpret the criteria. The Economist Intelligence Unit (EIU) published further "guidelines" in August 2013, to which we will refer.

The AGB set out 4 criteria, worth a score of 4 points each. These criteria were divided into subparts carrying various scores. An applicant was required to score 14 points out of the possible 16 to prevail in this evaluation

Criterion 1 is entitled "Community establishment", and is divided into 2 components A -"Delineation" and B - Extension". The criteria for these are set out at page 4-10, and then the definition section follows. The very first definition that is required to be understood and applied to the criterion is whether or not there is a community involved in the application. That definition comes first, and logically is a pre-requisite to the later steps of seeing how well delineated that community is, or how old it is, etc. The first question that has to be asked is "Is there a community that meets the definition of "community" under these rules"? If there is not, then the rest of the analysis is unnecessary, as the applicant should fail at the first hurdle.

The Panel did not attempt this analysis, in breach of the requirements of the policy and process for CPE.

The definition of community begins by noting that it means more than its Latin origins in "*communitas*" meaning fellowship, but observing that it still implies "more of cohesion than a mere commonality of interest". Not testing whether there was a community at all under this definition is critical, as it is readily apparent from the evidence and the application text that a "mere commonality of interest" is precisely what links the applicant and its supporters, without any of the "cohesion" that a true community under this definition must have. This is not a disagreement about a finding by the Panel on this topic; the Panel did not consider this definition, nor apply the test for "community" required.

The definitions of "community" go on to refer to 3 further conditions that must be satisfied for a finding that a community existed.

They are:

(2) an awareness and recognition of a community among its members;
(3) some understanding of the community's existence prior to September 2007 (when the new gTLD policy recommendations were completed); and
(4) extended tenure or longevity—non-transience—into the future.

The Panel did refer to these definitions, but failed to consider the first and vital question of whether there was first a cohesive community, bound together by more than a mere commonality of interest. Had it considered the matter, it would have appreciated that the applicants definition, rather than showing cohesion, depended instead on coercion; every hotelier is deemed a member of this community, even though they have never heard of it, and would not chose to join it if asked, but are nevertheless deemed to be a member of it. Compulsory membership, and deemed memberships seem to be the opposite of the kind of community that is worth of the protection and reward of the

CPE process. However, as the Panel has simply omitted to consider cohesiveness, the matter can be reconsidered.

Failure to consider self-awareness and recognition of the community

The Panel report begins with the Panel being confused or mistaken about the criteria for the first criterion – Delineation. It says:

"Delineation
Two conditions must be met to fulfill the requirements for delineation: there must be a clear, straightforward membership definition, and there must be awareness and recognition of a community (as defined by the applicant) among its members."

In fact, the requirements of delineation are (in summary) that it must (1) be clearly delineated, (2) be organized, and (3) be pre-existing before 2007. The Panel got one out of the three requirements correct.

It will be observed that the Panel has imported the test for determining whether there is a "community" – self-awareness that the group is a community - into the test for "delineation". With respect, that is an error of process that further invalidates the findings.

Even if it were not, and self awareness and recognition are considered with Delineation, the actual response given under that enquiry about "self awareness and recognition" shows that the Panel does not understand the test that is to be applied. The response given by the Panel: "*This is because the community is defined in terms of its association with the hotel industry and the provision of specific hotel services.*" is a response directed only at the delineation issue, which is how the Panel posed the question, not as part of the "self-awareness" and "beyond mere commonality of interest" tests that goes into the definition of community. The Panel has not considered, and has therefore not concluded that the community has the requisite self-awareness and self-recognition to be a community for the purposes of CPE.

We observe, for the record, that the above quote is an almost meaningless statement even in the context of discussing delineation. The phrase is substantially repeated in relation to community longevity, where it is equally meaningless.

What is required is a showing by evidence that members of the alleged community regard themselves as members of a defined community, which is recognised as such by the members, and by people outside the community. Simply operating a hotel anywhere in the world might make one a member of the same trade, having a similar common interest. Once cannot declare that even hoteliers who have never heard of the associations supporting this applicant, operating in different countries from where these associations operate, are nevertheless members of a community with them, simply because they are in the same trade, and because there is an ISO definition of what a hotel is.

This is a very important issue for the AGB itself, which noted in its Guidelines:
*All (*referring to possible types of communities*) are viable as such, provided the requisite awareness and recognition of the community is at hand among the members. Otherwise the application would be seen as not relating to a real community and score 0 on both Delineation and Extension*

We invite the BGC to find that this is a failure to consider the issue of self-awareness and recognition, which does not arise from "association with the hotel industry" or "provision of hotel services" at all. That is, there has not been a consideration of the issue of self-awareness and recognition, if the response is on an entirely separate and distinct matter.

It is important to note that the Panel finds that the alleged community is clearly delineated, because there is an ISO definition of "hotel", and because every hotel is a member of the alleged community. The Panel says: *'The string "Hotel" is an internationally agreed word that has a clear definition of its meaning: According to DIN EN ISO 18513:2003, "A hotel is an establishment with services and additional facilities where accommodation and in most cases meals are available."* [3]

The Panel then proceeds through the proper requirements of Delineation, which it names accurately – organisation and existence before 2007.

Failure to apply test for Uniqueness

The next major consideration is that of Nexus- the link between the string and the purported Community. This is broken down in 2 parts: Nexus, worth 3 points and Uniqueness worth one point. To get 3 points under Nexus an applicant has to show that the string is either

(a) an exact match of the community name, or

(b) is a well know short form of the community name, or

(c) is an abbreviation of the community name.

An applicant who cannot score 3 points under those options, can score 2 points if it can show that the string "identifies" the community – but in a way that does not equate with the 3 conditions above. "Identify" is defined in the AGB as meaning *"...that the applied for string closely describes the community or the community members, without over-reaching substantially beyond the community".*

The AGB Guidelines say on this: *"With respect to "Nexus," for a score of 3, the essential aspect is that the applied-for string is commonly known by others as the identification / name of the community."*

Uniqueness is defined in the AGB as where the *"String has no other significant meaning beyond*

[3] There is some confusion in the Application itself, which defines hotels by reference to the ISO definition then appears to hold that the "establishments" themselves are members of the Community. For present purposes we proceed on the basis that while a hotel may be a defined establishment, the alleged community is made up of the people and enterprises that run the hotels, and also the associations that such people form among themselves.

identifying the community described in the application."

The Panel reports that the Applicant scored 2 points on Nexus, as the sting "identifies" the community. It explained itself thus: *"The string nexus (sic) closely describes the community, without overreaching substantially beyond the community. The string identifies the name of the core community members (i.e. hotels and associations representing hotels)."*

We observe that there is no evidence put forward for this claim, which remains an unsupported assertion by the Applicant, and that no web searches are reported, as recommended by the EIU to explore the issue. In particular, no evidence is given of how non-members of the community regard the string, and whether or not they associate the string "hotel" with the community of hoteliers seeking the TLD. It is manifestly obvious that it is also wrong in fact; the word "hotel" describes a place for obtaining lodging, not the hoteliers (Marriott, Sheraton, Crowne Plaza) and not their trade associations (IH&RA, HotRec, GHA).

The Panel then considered "Uniqueness".
It held: *"The Community Priority Evaluation panel determined that the application met the criterion for Uniqueness as specified in section 4.2.3 (Community Priority Evaluation Criteria) of the Applicant Guidebook, as the string has no other significant meaning beyond identifying the community described in the application."*

We remind the BGC that the Panel has itself already cited, and relied upon a definition of the string that has a meaning significantly different than the one just quoted. In determining that there was a delineated community, the Panel relied on the ISO definition of "hotel" – namely: *'The string "Hotel" is an internationally agreed word that has a clear definition of its meaning: According to DIN EN ISO 18513:2003, "A hotel is an establishment with services and additional facilities where accommodation and in most cases meals are available." '*

Patently, the word "hotel" has another "significant meaning" apart from identifying a community – it means a place where a customer can purchase lodgings.

The Panel has not followed ICANN policy or process in arriving at the conclusion that the string has "no other significant meaning beyond identifying the community" because it has itself cited a significant other meaning, and relied on that other meaning (that the word means "an establishment with services and additional facilities where accommodation and in most cases meals are available") in order to measure and find Delineation.

This is not a disagreement about a conclusion – this is a demonstration of a failure of process by the Panel. It cannot use the significant meaning of "hotel" under an ISO definition for one purpose (a finding under delineation), then deny that meaning and say there is "no other significant meaning" for the purposes of finding Uniqueness.

The point is an obvious one. There is no demonstrated "community", merely a business association of traders from the developed world with a common business interest. They wish to defeat the kind of competition and innovation that the ICANN program was intended to stimulate. The word

"hotel" means to most of the world what the ISO definition says it means- a place for lodging and meals. To assert that it means to most people the association of business enterprises that run the hotels is unsubstantiated and absurd.

Breaches of other ICANN Principles

Under Article 7 of the Affirmation of Commitments *"ICANN commits to provide a thorough and reasoned explanation of decisions taken, the rationale thereof and the sources of data and information on which ICANN relied."*

Under Article 1, Mission and Core Values of the ICANN Bylaws (11 Apr. 2013) at Clause 2.8 ICANN commits to the core value of *"Making decisions by applying documented policies neutrally and objectively, with integrity and fairness."*

Under Article III, Section 1 of the Bylaws ICANN commits: *"ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness."*

Under Article IV, Clause 2.20, the purpose of Reconsideration is to:*"...to ensure that all persons materially affected by ICANN decisions have meaningful access to a review process that ensures fairness while limiting frivolous claims."*

Requestor submits that various aspects of the CPE process breach, or risk breaching, these fundamental provisions. All of the members of the Requestor group (and there are others) are competing applicants for the .hotel TLD. CPE is a process by which all were "materially affected" but in which a number of elements of basic fairness seem to be lacking. Although CPE is not set up as an *inter partes* contest, there are a number of features which are prejudicial to standard applicants, including:

(a) Insufficient material was made available to them as to who the Panelist was, and their qualifications. Several instances of possible conflict of interest involving Dispute Resolution Providers have arisen during the course of the new gTLD rollout to date. The way to ensure there is no criticism of the process, and to prevent actual conflicts is to ensure full notification of all details is provided to affected parties.

(b) There is no publication of the materials to be examined by the Panel. It is possible for the Panel to request further information during CPE, but it is not clear whether any, and if so what, material was sought and what was provided. Communications made between the Applicant and the CPE panel during the evaluation process should be made public. In relation to any such material, standard applicants should have some way of providing counter balancing material for the panel's consideration.

(c) Insufficient analysis and reasons were given on how the Panelist reached their decision in the CPE report: (http://www.icann.org/sites/default/files/tlds/hotel/hotel-cpe-1-1032-95136-en.pdf). By way of example, a crucial issue in CPE is the whether or not there is a self-aware, well recognized

"hotel community" entitled to the special privileges that the AGB provides.

Far from providing the "*thorough and reasoned explanation of decisions taken, the rationale thereof and the sources of data and information on which ICANN relied.*" On this crucial issue the Panel says only this:

"*This is because the community is defined in terms of its association with the hotel industry and the provision of specific hotel services.*"

This is relatively nonsensical in the context of an allegedly global community. No evidence for the existence of this community was provided at all. Given the importance of this finding, and the impact on the affected parties, a thorough rationale should be provided, with the sources of data and information relied upon spelled out.

While the BGC takes the apparent view that the quality of decision-making is not available for reconsideration, the parties are denied "*...meaningful access to a review process that ensures fairness while limiting frivolous claims.*" Simply noting that the Panel has asked the question that the AGB requires, without regard to whether the answer has any relevance to the question posed is not reconsideration, and is not a fair assessment of whether ICANN polices and processes have been applied *neutrally and objectively, with integrity and fairness.*

9. What are you asking ICANN to do now?

Requester requests that the current finding that the Applicant has prevailed in CPE should be set aside. The Application should be remitted to the Panel for re-examination, with the Panel directed to have regard to the matters raised in the reconsideration request, and any further direction from the BGC. [JN: Should we ask for the necessary information here or do a separate info request?]

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

Requestor is a group of applicants in ICANN new gTLD program. Each of the members of the group is affected by the finding in CPE of which Reconsideration is sought

11. Are you bringing this Reconsideration Request on behalf of multiple persons or entities? (Check one)

___X_ Yes

____ No

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

Yes

Explain.

The parties are members of the same contention set, all being applicants for a .hotel TLD

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

No

Terms and Conditions for Submission of Reconsideration Requests

The Board Governance Committee has the ability to consolidate the consideration of Reconsideration Requests if the issues stated within are sufficiently similar.

The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious.

Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing.

The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC.

The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.

Jay Westerdal 6/28/2014

Signature Date

crowell moring

Annex 10.

For the a ention of Mr Cherine Chalaby

Chair, ICANN New gTLD Program Committee

Document Information Disclosure Policy Request

By email: didp@icann.org

4th August 2014

Dear Sir,

Pursuant to ICANN's Documentary Information Disclosure Policy ("DIDP"), the applicants for the .HOTEL gTLD named at the end of this le er or their advisers hereby request the documents described further in this le er.

Relevant Background

On 11 June 2014, ICANN issued a Community Priority Evaluation Report ("Report") which determined that the Community Application ("CPE Application") by HOTEL Top-Level-Domain s.a.r.l. (Application I.D. 1-1032-95136) ("Hotel TLD") for the .HOTEL string had been successful.

The surprising success of the CPE Application leaves open the question of whether the correct standards of due care were applied, as the Report itself was largely perfunctory and made scarce reference to the underlying reasoning and documentation relied on by the Community Priority Evaluation Panel ("CPE Panel").

The Applicants, therefore, hereby respectfully request that ICANN produce the following documents directly and indirectly relating to the Report:

1) All correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication ("Communications") between individual member of ICANN's Board or any member of ICANN Staff and the Economist Intelligence Unit or any other organisation or third party involved in the selection or organisation of the CPE Panel for the Report, relating to the appointment of the Panel that produced the Report, and dated within the 12 month period preceding the date of the Report;
2) The curriculum vitaes ("CVs") of the members appointed to the CPE Panel;
3) All Communications (as defined above) between individual members of the CPE Panel and/or ICANN, directly relating to the creation of the Report; and
4) All Communications (as defined above) between the CPE Panel and/or Hotel TLD or any other party prior with a material bearing on the creation of the Report.

("Requested Information"

The Requested Information does not meet any of the defined conditions under the DIDP for non-disclosure, and we consider each of these in turn:

- *Information provided by or to a government or international organization, or any form of recitation of such information, in the expectation that the information will be kept confidential and/or would or likely would materially prejudice ICANN's relationship with that party.*

  This condition does not apply.

- *Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.*

  Disclosure of the Requested Information would clearly promote the integrity of ICANN's deliberati e and decision making process because all applicants for new gTLDs are reliant on the principles of fairness and transparency as the two pillars which enshrine and ensure that the process which they have subscribed to is completely conducted in good faith. There can be no justi ation for secrecy in relation to what is e ecti ely a quasi-judicial process.

In addition we note, for the avoidance of doubt:

1) The Requested Information is unrelated to any personal, medical, contractual, remuneration or similar records.

2) The Requested Information is not likely to impermissibly prejudice any parties' commercial, financial or competi e interests. Additionally, to the extent that any requested document contains such information, the Requested Information should be redacted accordingly before it is provided in response to this request.

3) The Requested Information is not confide tial business information or internal policies or procedures.

4) The Requested Information will not endanger the life, health or safety of any individual nor prejudice the administration of justice

5) The Requested Information is not subject to a orney-client privilege.

6) The Requested Information is not drafts of communications

7) The Requested Information is not related in any way to the security or stability of the Internet.

8) The Requested Information is not trade secrets or financial information

9) The Requested Information request is reasonable, not excessive or overly burdensome, compliance is feasible and there is no abuse.

To the extent that any of the Requested Information does fall into one of the defined conditions for non-disclosure, ICANN should nonetheless disclose the information as the public interest in disclosing the informatiaon outweighs any harm that might be caused by disclosure.

ICANN's transparency obligations, created in ICANN's bylaws[1] and Articles of Incorporatio [2], require publication of information related to the process, facts and analysis used by individual members of the CPE Panel in preparation of the Report.

Bylaw Article III, Section 1 provides as follows: "ICANN and its constitue t bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness."

---

1 (http:// ww.icann.org/general/bylaws.htm#I)

2 htt s://www.icann.org/resources/pages/articles-2012-02-25-e

Article I, Section 2 of the ICANN Bylaws also state that in performing its mission, a set of core values should guide the decisions and actions of ICANN. These include:

7. Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most a ected can assist in the policy development process.

8. Making decisions by applying documented policies neutrally and objectively, with integrity and fairness.

9. Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most a ected.

10. Remaining accountable to the Internet community through mechanisms that enhance ICANN's e ecti eness.

Article 4 of the ICANN Articles of Incorporation provides:

"The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this e ect, the Corporation shall cooperate as appropriate with relevant international organizations "

The ICANN community and certainly the Applicants are entitled to know both the qualifications and details of the appointment of members of the CPE Panel that made the decision and how they applied the relevant standards and the material on which they relied, following which the CPE Application of Hotel TLD for the .HOTEL string was successful, as the issue is causing enormous concern in the community.

Yours faithfully,

Jonathon Nevett

Donuts Inc

FairWinds Partners, LLC

~~Fegistry LLC~~

Fegistry LLC

~~FairWinds Partners~~

Famous Four Media Limited (on behalf of dot Hotel Limited)

Minds + Machines

Radix FZC

crowell moring

Annex 11.

DETERMINATION

OF THE BOARD GOVERNANCE COMMITTEE (BGC)

RECONSIDERATION REQUEST 14-34

22 AUGUST 2014

Despegar Online SRL, DotHotel, Inc., dot Hotel Limited, Fegistry, LLC, Spring McCook, LLC and Top Level Domain Holdings Limited (collectively, the "the Requesters") seek reconsideration of the Community Priority Evaluation Panel's Report ("Report"), and ICANN's acceptance of that Report, finding that HOTEL Top-Level-Domain S.a.r.l.'s application for .HOTEL prevailed in Community Priority Evaluation ("CPE").

I. Brief Summary.

All six Requesters applied for .HOTEL. HOTEL Top-Level-Domain S.a.r.l. ("Applicant") also applied for .HOTEL as a community applicant. All seven .HOTEL applications were placed into a contention set. Having submitted the only community application for .HOTEL, the Applicant was invited to and did participate in a CPE for .HOTEL. On 12 June 2014, the Application prevailed in CPE. The Requesters now claim the CPE Panel ("Panel") failed to comply with established ICANN policies and procedures in rendering its Report. Specifically, the Requesters contend the Panel: (i) improperly interpreted and applied the CPE criteria set forth in the New gTLD Applicant Guidebook ("Guidebook"); and (ii) breached "other ICANN [p]rinciples" set forth in the ICANN Bylaws. (Request, § 8, Pgs. 5-11.)

The Requesters' claims are unsupported. First, while the Request is couched in terms of the Panel's purported violations of various procedural requirements, the Requesters do not identify any misapplication of a policy or procedure, but instead challenge the merits of the Panel's Report, which is not a basis for reconsideration. Second, the Requesters' allusions to the

broad fairness principles expressed in ICANN's Bylaws cannot serve as a basis for reconsideration, as the Requesters do not identify any specific Panel action that contravenes those principles. Because the Requesters have failed to demonstrate that the Panel acted in contravention of established policy or procedure, the BGC denies Request 14-34.

II. Facts.

A. Background Facts.

All six Requesters applied for .HOTEL.

The Applicant filed a community application for .HOTEL (*i.e.*, a seventh application for .HOTEL).

On 19 February 2014, the Applicant was invited to participate in the CPE process for .HOTEL. The Applicant elected to participate in the process, and its .HOTEL community application ("Application") was forwarded to the CPE Panel assembled by the Economist Intelligence Unit ("EIU").

On 11 June 2014, the Panel issued its Report. The Panel determined the Application met the requirements specified in the Guidebook and therefore concluded that the Application prevailed in the CPE. Because the Application prevailed in CPE, each of Requesters' applications in the .HOTEL contention set will not proceed. (*See* Guidebook, § 4.2.3.)

On 12 June 2014, ICANN posted the Report on its microsite.

On 28 June 2014, the Requesters filed Request 14-34, requesting reconsideration of the Panel's determination that the Application prevailed in CPE.[1]

[1] Reconsideration Requests must be filed within 15 days of "the date on which the party submitting the request became aware of, or reasonably should have become aware of, the challenged staff action." Bylaws, Art. IV, § 2.5.b. Requesters arguably "should have become aware of" the CPE Panel's Report on 12 June 2014, the day it was publicly posted, in which case Requesters Reconsideration Request – which was submitted on 28 June 2014 – is untimely. However, because the Requesters represent that they did not in fact become aware of the CPE Panel's Report until 13 June 2014, the BGC will consider the Request on the merits.

B. The Requesters' Claims.

The Requesters contend that the Panel failed to comply with ICANN policies and procedures in two ways. First, the Requesters claim "there are three instances where the Panel has not followed the AGB policy and processes for conducting the CPE." (Request, § 8, Pg. 5.) Second, the Requesters claim "the Panel, and ICANN staff, have breached more general ICANN policies and procedures in the conduct of this CPE." (Request, § 8, Pg. 5.)

C. Relief Requested.

The Requesters suggest "that the current finding that the Applicant has prevailed in CPE should be set aside . . . [and] should be remitted to the Panel for re-examination, with the Panel directed to have regard to [*sic*] the matters raised in the reconsideration request[.]" (Request, § 9, Pg. 11.)

III. Issues.

In view of the claims set forth in Request 14-34, the issues are whether the Panel acted in contravention of established policy or procedure by:

A. Improperly applying the criteria set forth in the Guidebook in determining that the Application prevailed in CPE; and

B. Violating other ICANN policies and procedures by: (i) providing insufficient information regarding the Panel's qualifications; (ii) failing to publicly post communications that might have taken place between the Panel and the Applicant; or (iii) providing insufficient analysis of the Panel's determination.

IV. The Relevant Standards for Evaluating Reconsideration Requests and Community Priority Evaluation.

ICANN's Bylaws provide for reconsideration of a Board or staff action or inaction in

accordance with specified criteria.[2] (Bylaws, Art. IV, § 2.) Dismissal of a request for reconsideration of staff action or inaction is appropriate if the BGC concludes, and the Board or the NGPC[3] agrees to the extent that the BGC deems that further consideration by the Board or NGPC is necessary, that the requesting party does not have standing because the party failed to satisfy the reconsideration criteria set forth in the Bylaws. ICANN has previously determined that the reconsideration process can properly be invoked for challenges to expert determinations rendered by panels formed by third party service providers, such as the EIU, where it can be stated that the Panel failed to follow the established policies or procedures in reaching its determination, or that staff failed to follow its policies or procedures in accepting that determination.[4]

In the context of the New gTLD Program, the reconsideration process does not call for the BGC to perform a substantive review of CPE reports. Accordingly, the BGC does not evaluate the Panel's substantive conclusion that the Applicant prevailed in the CPE. Rather, the BGC's review is limited to whether the Panel violated any established policy or process, which the Requesters suggest was accomplished when the Panel: (i) purportedly misapplied the CPE

---

[2] Article IV, § 2.2 of ICANN's Bylaws states in relevant part that any entity may submit a request for reconsideration or review of an ICANN action or inaction to the extent that it has been adversely affected by:

(a) one or more staff actions or inactions that contradict established ICANN policy(ies); or
(b) one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act; or
(c) one or more actions or inactions of the ICANN Board that are taken as a result of the Board's reliance on false or inaccurate material information.

[3] New gTLD Program Committee.

[4] *See* http://www.icann.org/en/groups/board/governance/reconsideration/recommendation-booking-01aug13- en.doc, BGC Recommendation on Reconsideration Request 13-5.

criteria set out in the Guidebook; and (ii) violated core ICANN principles set forth in its Bylaws. (Request, § 8, Pg. 5.)

The standards governing CPE are set forth in Section 4.2 of the Guidebook. In addition, the EIU – the firm selected to perform CPE – has published supplementary guidelines ("CPE Guidelines") that provide more detailed scoring guidance, including scoring rubrics, definitions of key terms, and specific questions to be scored.[5]

CPE will occur only if a community-based applicant selects this option and after all applications in the contention set have completed all previous stages of the process. (Guidebook, § 4.2.) Community priority evaluations will be performed by an independent community priority panel appointed by EIU to review these applications. (*See* Guidebook, § 4.2.2.) The panel's role is to determine whether any of the community-based applications fulfills the four community priority criteria set forth in Section 4.2.3 of the Guidebook. The four criteria include: (i) community establishment; (ii) nexus between proposed string and community; (iii) registration policies; and (iv) community endorsement. To prevail in a CPE, an application must receive a minimum of 14 points on the scoring of foregoing four criteria, each of which is worth a maximum of four points (for a maximum total of 16 points).

V. Analysis and Rationale.

The Requesters have failed to demonstrate that the Panel violated any established policy or procedure in rendering the Report.

1. The Panel Properly Applied the CPE Criteria.

[5] The CPE Guidelines may be found here: http://newgtlds.icann.org/en/announcements-and-media/announcement-27sep13-en.

The Requesters identify three ways in which the Panel allegedly failed to apply the Guidebook criteria. First, the Requesters claim the Panel did not analyze whether a "community," as that term is defined in the Guidebook, has been identified. Second, the Requesters argue the Panel was "confused or mistaken" about the criteria required to support a finding that the community is sufficiently delineated. Third, the Requesters assert the Panel failed to apply the Guidebook's test for uniqueness. (Request, § 8, Pgs. 6-11.) As discussed below, the Requesters have provided no support for their contention that the Panel incorrectly applied any policy or procedure.

(a) The Panel Properly Analyzed Whether The "Hotel Community" Meets the Guidebook Definition of a Community.

Guidebook section 4.2.3 sets forth the requirements for "Community Establishment." It states that whether an Applicant has established a "community" for CPE purposes will be "measured by" two factors: delineation and extension. In addition, Guidebook section 4.2.3 provides:

> [A]s "community" is used throughout the application, there should be: (a) an awareness and recognition of a community among its members; (b) some understanding of the community's existence prior to September 2007 (when the new gTLD policy recommendations were completed); and (c) extended tenure or longevity—non-transience—into the future.

The Requesters concede the Panel "did refer to these definitions" (Request, § 8, Pg. 6), but contend the Panel erred in failing to "consider the first and vital question of whether there was first a cohesive community" separate and apart from the specified above-listed criteria. (Request, § 8, Pg. 6.) However, the Requesters point to no obligation to conduct any inquiry as to the definition of a community other than those expressed in section 4.2.3 of the Guidebook, which Requesters admit the Panel took into account. As such, the Requesters fault the Panel for adhering to the Guidebook's definition of a "community" when evaluating the Application.

Given that the Panel must adhere to the standards laid out in the Guidebook, this ground for reconsideration fails.

The Requesters also contend the Applicant's proposed community, *i.e.,* the "Hotel Community," does not qualify as a community for CPE purposes because "rather than showing cohesion, [it] depend[s] on coercion; every hotelier is deemed a member of this community, even if they have never heard of it[.]" But the Panel reached the contrary conclusion, noting "the community as defined in the application has awareness and recognition among its members. This is because the community is defined in terms of its association with the hotel industry and the provision of specific hotel services." (Report, Pg. 2.) As even the Requesters note, a request for reconsideration cannot challenge the substance of the Panel's conclusions, but only its adherence to the applicable policies and procedures. Accordingly, reconsideration is not warranted based on the Requesters' complaint that the Panel came to a different conclusion than Requesters' would have liked as to whether the Hotel Community enjoys sufficient recognition amongst its members.

(b) The Panel Properly Applied the Test for Delineation.

Guidebook section 4.2.3 provides that delineation "relates to the membership of a community," and that membership must be "[c]learly delineated, organized, and pre-existing [the completion of the new gTLD policy recommendations in 2007]." The Requesters contend the Panel committed an "error of process" because it "imported the test for determining whether there is a 'community' . . . into the test for 'delineation.'" (Request, § 8, Pg. 7.) Specifically, the Requesters fault the Panel for purportedly ignoring the requirements that the community be organized and preexisting before 2007. (*Id*.) The Requesters' claim is unsupported, as the Report shows that the Panel fully examined all three requirements for delineation.

The Panel began its assessment of the test for delineation by noting: "Two conditions must be met to fulfill the requirements for delineation: there must be a clear, straightforward membership definition, and there must be awareness and recognition of a community (as defined by the applicant) among its members." (Report, Pg. 1.) As the Requesters admit, the Panel then "proceeds through the proper requirements of Delineation, which it names accurately[.]" (Request, § 8, Pg. 8.) The Requesters thus defeat their own argument, as they squarely concede the Panel assessed the "proper requirements" of the test for delineation.

Again, the Requesters dispute the Panel's allusion to the "awareness and recognition" of the Hotel Community's members not because that reference constitutes any procedural violation, but because the Requesters simply disagree whether there is any such recognition amongst the Hotel Community's members. In fact, in the same section where they fault the Panel for considering self-awareness in the process of the delineation inquiry, the Requesters also complain of the Panel's purported "failure to consider the issue of self-awareness and recognition." (Request, § 8, Pg. 8.) At bottom, the Requesters do not challenge how and when the Panel applied either the delineation or self-awareness tests, but instead seek reconsideration of the substance of the Panel's determination that the Hotel Community is clearly delineated and its members are sufficiently self-aware. Disagreement with the Panel's substantive conclusions, however, is not a proper basis for reconsideration.

(c) The Panel Properly Applied the Test for Uniqueness.

The second criterion by which the Application is assessed in CPE is the nexus between the proposed string and the community. (Guidebook, § 4.2.3.) This criterion evaluates "the relevance of the string to the specific community that it claims to represent" through the scoring of two elements—2-A, nexus (worth three points), and 2-B, uniqueness (worth one point). (Guidebook, § 4.2.3.) To fulfill the requirements for element 2-B, the string must have "no other

significant meaning beyond identifying the community described in the application." (Guidebook, § 4.2.3.)

Here, the Panel concluded that .HOTEL "has no other significant meaning beyond identifying the community described in the application." (Report, Pg. 4.) The Panel cited the Application's definition of "hotel" as "an establishment with services and additional facilities where accommodation and in most cases meals are available." (Request, § 8, Pg. 9; Report, Pg. 2.) The Requesters contend the Panel erred in so finding because "[p]atently, the word 'hotel' has another 'significant meaning' apart from identifying a community – it means a place where a customer can purchase lodgings." (Request, § 8, Pg. 9.) In other words, the Requesters claim that the string .HOTEL has a significant meaning apart from identifying the Hotel Community, because it claims the Hotel Community is an "association of business enterprises that run the hotels," whereas the word "'hotel' means to most of the world what the [Application's] definition says it means – a place for lodging and meals." (Request, § 8, Pgs. 9-10.)

The Requesters have identified no procedural deficiency in the Panel's determination that the uniqueness requirement was met. The Requesters concede that "HOTEL" has the significant meaning of a place for lodging and meals, and common sense dictates that the Hotel Community consists of those engaged in providing those services. The attempt to distinguish between those who run hotels and hotels themselves is merely a semantic distinction. Again, while the Requesters may disagree with the Panel's substantive conclusion, that is not a proper basis for reconsideration. The Requesters do not identify any Guidebook or other procedural requirement that the Panel purportedly violated in reaching its determination that "HOTEL" has the significant meaning of a place for lodging and meals, and the Requesters arguments that the finding was erroneous do not form the grounds for a reconsideration request.

2. The Panel Did Not Breach Any Provisions of the ICANN Bylaws.

The Requesters argue that three aspects of the CPE process violate core ICANN values of promoting fair and transparent decision-making. (Request, § 8, Pgs. 10-11 (citing ICANN Bylaws, Art. 1, § 2.8; *id*., Art. III, § 1; *id*., Art. IV, § 2.2; ICANN Affirmation of Commitments, Art. 7).) In particular, the Requesters argue the CPE process is "prejudicial to standard applicants" because: (1) the standard applicants are not given enough information regarding the identity or qualifications of the Panelist to assess potential conflicts; (2) the materials considered by the Panel are not publicly posted; and (3) the Panel provided insufficient "analysis and reasons" for its conclusions.

None of these concerns represent a policy or procedure violation for purposes of reconsideration under ICANN's Bylaws. The Guidebook does not provide for any of the benefits that the Requesters claim they did not receive during CPE of the Application. In essence, the Requesters argue that because the Guidebook's CPE provisions do not include Requesters' "wish list" of procedural requirements, the Panel's adherence to the Guidebook violates the broadly-phrased fairness principles embodied in ICANN's foundational documents. Were this a proper ground for reconsideration, every standard applicant would have the ability to rewrite the Guidebook via a reconsideration request. Such a result would undermine the stability of the New gTLD Program and ICANN's accountability mechanisms. ICANN's general commitment to fairness and transparency cannot form a basis for reconsideration here because the Guidebook simply does not confer upon standard applicants the benefits that the Requesters complain they did not receive, and reconsideration is only warranted where a staff action "contradict[s] *established* ICANN policy(ies)[.]" (Bylaws, Art. IV, § 2, emphasis added.) Moreover, the Guidebook was extensively vetted by the ICANN stakeholder community over a course of years and included a total of ten versions with multiple notice and public comment

periods.[6] To stray from the Guidebook's terms and impose additional requirements, as the Requesters would have the BGC do here, would violate many of the very same fairness principles the Requesters invoke.[7]

VI. Determination.

Based on the foregoing, the BGC concludes that the Requesters have not stated proper grounds for reconsideration, and therefore denies Reconsideration Request 14-34. Given that there is no indication that the Panel violated any policy or procedure in reaching, or staff in accepting, the conclusions in the Panel's Report, this Request should not proceed. If the Requesters believe they have somehow been treated unfairly in the process, the Requesters are free to ask the Ombudsman to review this matter.

In accordance with Article IV, § 2.15 of the Bylaws, the BGC's determination on Request 14-34 shall be final and does not require Board consideration. The Bylaws provide that the BGC is authorized to make a final determination for all Reconsideration Requests brought regarding staff action or inaction and that the BCG's determination on such matters is final. (Bylaws, Art. IV, § 2.15.) As discussed above, Request 14-34 seeks reconsideration of a staff action or inaction. After consideration of this Request, the BGC concludes that this determination is final and that no further consideration by the Board (or the New gTLD Program Committee) is warranted.

---

[6] The current version of the Guidebook is available at http://newgtlds.icann.org/en/applicants/agb. The prior versions of the Guidebook are available at http://newgtlds.icann.org/en/about/historical-documentation. As noted in its Preamble, the Guidebook was the product of an extensive evaluation process that involved public comment on multiple drafts.

[7] Moreover, any challenge to the terms of the current version of the Guidebook are untimely, as more than fifteen days have elapsed since it was promulgated in June 2012. (*See* Bylaws, Art. IV, § 5 (setting forth fifteen day deadline to file reconsideration request after challenged action.)

In terms of the timing of this decision, Section 2.16 of Article IV of the Bylaws provides that the BGC shall make a final determination or recommendation with respect to a Reconsideration Request within thirty days following receipt of the request, unless impractical. (*See* Bylaws, Article IV, § 2.16.) To satisfy the thirty-day deadline, the BGC would have to have acted by 28 July 2014. Due to the volume of Reconsideration Requests received within recent months, it was impractical for the BGC to consider Request 14-34 prior to 22 August 2014.

crowell moring

Annex 12.

Response to Documentary Information Disclosure Policy Request

To: Donuts, Inc.; FairWinds Partners, LLC; Fegistry LLC; Famous Four Media Limited; Minds + Machines; and Radix FZC

Date: 3 September 2014

Re: Request No. 20140804-1

Thank you for your Request for Information dated 4 August 2014 (the "Request"), which was submitted through the Internet Corporation for Assigned Names and Numbers' ("ICANN's") Documentary Information Disclosure Policy ("DIDP"). For reference, a copy of your Request is attached to the email forwarding this Response.

Items Requested

In summary, the Request seeks all communications relating to the creation of the Community Priority Evaluation ("CPE") report (the "Report") approving the community application for .HOTEL submitted by HOTEL Top-Level-Domain S.a.r.l. ("Hotel TLD") and relating to the appointment of the CPE Panel that produced the Report. The Request identified certain specific categories of documents, including:

1. All correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication ("Communications") between individual member [*sic*] of ICANN's Board or any member of ICANN Staff and the Economist Intelligence Unit or any other organization or third party involved in the selection or organization of the CPE Panel for the Report, relating to the appointment of the Panel that produced the Report, and dated within the 12 month period preceding the date of the Report;

2. The curriculum vitaes ("CVs") of the members appointed to the CPE Panel;

3. All Communications (as defined above) between individual members of the CPE Panel and/or ICANN, directly relating to the creation of the Report; and

4. All Communications (as defined above) between the CPE Panel and/or Hotel TLD or any other party prior with a material bearing on the creation of the Report.

Response

The Community Priority Evaluation ("CPE") standards set forth in Section 4.2 of the Applicant Guidebook ("Guidebook") available at http://newgtlds.icann.org/en/applicants/agb. CPEs are performed by an independent community panel that is coordinated by the Economist Intelligent Unit ("EIU"), an independent, third-party company that contracts with ICANN to perform that coordination role. The CPE Panel Process Document (at http://newgtlds.icann.org/en/applicants/cpe) and the CPE Guidelines (at

http://newgtlds.icann.org/en/applicants/cpe) provide more information on the CPE process.

To help assure independence of the process and evaluation, ICANN (either Board or staff) is not involved with the selection to the CPE panel of the two individual evaluators that perform the scoring in each CPE process (the "CPE Panel"), nor is ICANN provided with information about who the evaluators on any individual panel may be. The coordination of the CPE Panel as explained in the CPE Panel Process Document, is performed entirely within the EIU. ICANN therefore does not have any CVs for the CPE Panel as requested in Item 2. Similarly, ICANN does not have documentation regarding the appointment of the specific CPE Panel for the .HOTEL CPE as requested in Item 1. To the extent that ICANN has documentation with the EIU for the performance of its role as the coordinating firm as it relates to the .HOTEL CPE, those documents are subject to certain of the Defined Conditions of Nondisclosure set forth in the DIDP:

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

- Confidential business information and/or internal policies and procedures.

- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

Item 3 seeks all Communications (as defined in the Request) between ICANN and the individual members of the CPE Panel relating to the creation of the Report. Because of the EIU's role as the panel firm, ICANN does not have any communications (nor does it maintain any communications) with the evaluators that identify the scoring for any individual CPE. As a result, ICANN does not have documents of this type. To the extent that ICANN has communications with persons from EIU who are not involved in the scoring of a CPE, but otherwise assist in a particular CPE, (as anticipated in the CPE

Panel Process Document), those documents are subject to the following Defined Conditions of Nondisclosure set forth in the DIDP:

- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

- Confidential business information and/or internal policies and procedures.

- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

Item 4 seeks all Communications between the CPE Panel and Hotel TLD or any other party bearing on the creation of the Report. In order to maintain the independence and neutrality of the CPE Panels as coordinated by the EIU, ICANN has limited the ability for requesters or other interested parties to initiate direct contact with the panels – the CPE Panel goes through a validation process regarding letters of support or opposition (as described in the CPE Panel Process document) but that is the extent of direct communications that the CPE Panel is expected to have. For process control purposes, from time to time ICANN is cc'd on the CPE Panel's verification emails. These validation emails are not appropriate for disclosure pursuant to the following Defined Conditions of Nondisclosure set forth in the DIDP:

- Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

In making its evaluation, the CPE Panel considers the application materials and other documentation, including letter(s) of support and relevant correspondence, from the public ICANN website and/or ICANN's New gTLD microsite, available at http://newgtlds.icann.org/en/. Correspondence regarding New gTLD applications is available at http://newgtlds.icann.org/en/program-status/correspondence, specific instances of correspondence regarding .HOTEL's CPE are available at https://www.icann.org/en/system/files/correspondence/levy-to-willett-03mar14-en.pdf,

https://www.icann.org/en/system/files/correspondence/sahjwani-to-chalaby-willett-04mar14-en.pdf, and https://www.icann.org/en/system/files/correspondence/patetta-to-icann-05mar14-en.pdf. In addition, the public is permitted to post comments regarding any New gTLD application on the New gTLD microsite. Several such comments were posted regarding .HOTEL and are available at https://gtldcomment.icann.org/applicationcomment/viewcomments, and the CPE Panel was obligated to take those into account. Similarly, the application that the CPE was based upon is available at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1165, with any updates available at https://gtldresult.icann.org/application-result/applicationstatus/applicationchangehistory/1562.

Although your analysis in the Request concluded that no Conditions for Nondisclosure should apply, ICANN must independently undertake the analysis of each Condition as it applies to the documentation at issue, and make the final determination as to whether any Nondisclosure Conditions apply. Here, for example, ICANN cannot violate contractual conditions that require ICANN to maintain items as confidential solely because the Request proffers that no such conditions apply. Similarly, ICANN does not release draft documentation – particularly if draft documentation was shared for the purpose of facilitating deliberations or decision making – because drafts are not reliable sources of information regarding what actually occurred or standards that were actually applied.

For each of the items identified above as subject to Defined Conditions of Nondisclosure, ICANN has determined that there are no particular circumstances for which the public interest in disclosing the information outweighs the harm that may be caused to ICANN, its contractual relationships and its contractors' deliberative processes by the requested disclosure.

About DIDP

ICANN's DIDP is limited to requests for information already in existence within ICANN that is not publicly available. In addition, the DIDP sets forth Defined Conditions of Nondisclosure. To review a copy of the DIDP please see https://www.icann.org/resources/pages/didp-2012-02-25-en. ICANN makes every effort to be as responsive as possible to the entirety of your Request.

We hope this information is helpful. If you have any further inquiries, please forward them to didp@icann.org.

crowell moring

Annex 13.

Reconsideration Request

Regarding Action Contrary to Established ICANN Policies
Pertaining to Community Objections to New gTLD Applications

Introductory Summary

i. The Requestors identified below, as parties "adversely affected by" an "ICANN action ... that contradict[s] established ICANN policy," respectfully submit this request for reconsideration ("Request") to the Board Governance Committee ("BGC"). Bylaws Art. IV § 2.2(a). Requestors ask the BGC to reconsider action by ICANN staff denying a request for production of documents ("RFP") made by Requestors pursuant to ICANN's Documentary Information Disclosure Policy ("DIDP"). The DIDP serves to implement ICANN's charge to "operate to the maximum extent feasible in an open and transparent manner … consistent with procedures designed to ensure fairness," *id.* Art. III § 1, and its refusal to honor the RFP betrays that founding principle.

ii. The RFP seeks information pertaining to a report ("Report") by an unidentified panel which performed a Community Priority Evaluation ("CPE") concerning a community-based application ("Application"), by HOTEL Top-Level-Domain s.a.r.l. ("Hotel TLD"), for the new generic top-level domain <.HOTEL> (the "String"). In its Report, the CPE panel concluded that the Application had satisfied the CPE criteria sufficiently to earn community priority. As a consequence, Requestors – each of which also had applied for the String – became excluded from competing for it.

iii. Dismayed by this result, Requestors undertook by their RFP to ascertain the identity and qualifications of the CPE panel, information regarding panelist selection, and the panelists' communications among themselves and/or with Hotel TLD or ICANN relating to or having any material bearing upon the Report. The RFP would determine, among other things, whether the anomalous CPE ruling resulted from improper selection or training of, or influence upon, the panel. Notwithstanding its commitment to transparency, fairness, independence and non-discrimination, ICANN attempts to shield

this important information from scrutiny by those directly and adversely affected by the CPE panel's decision. Reconsideration properly lies to remedy ICANN's obstinacy as contrary to its own documented policies.

1. Requestor Information

a. Name: Despegar Online SRL

Address: Contact Information Redacted

Email: Contact Information Redacted

b. Name: Radix FZC

Address: Contact Information Redacted

Email: Contact Informat on Redacted

c. Name: Famous Four Media Limited

Address: Contact Information Redacted

Email: Contact Information Redacted

d. Name: Fegistry, LLC

Address: Contact Information Redacted

Email: Contact Information Redacted

e. Name: Donuts Inc.

Address: Contact Information Redacted

Email: Contact Information Redacted

f. Name: Minds + Machines

Address: Contact Information Redacted

Email: Contact Information Redacted

The foregoing are referred to collectively herein as "Requestors." This Request is submitted on behalf of Requestors by:

Counsel: John M. Genga, Don C. Moody
The IP and Technology Legal Group, P.C.
dba New gTLD Disputes

Address: Contact Information Redacted

Email: Contact Information Redacted

2. Request for Reconsideration of:

_____ Board action/inaction

__X__ Staff action/inaction

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

3.1. Requestors seek reconsideration of ICANN's denial of the RFP. As a "principal element of ICANN's approach to transparency and information disclosure," the DIDP is "intended to ensure that information contained in documents concerning ICANN's operational activities … is made available to the public unless there is a compelling reason for confidentiality." *See* https://www.icann.org/resources/pages/didp-2012-02-25-en. ICANN's refusal to provide documents responsive to the RFP violates this policy and the transparency touted as a "core value" established to guide its actions. Bylaws Art. I § 7, Art. III § 1.

3.2. ICANN provided for reconsideration to remedy "staff actions" that so "contradict" such "established ICANN policies." *Id*. Art. IV § 2.2(a). It becomes acutely important where, as here, enforcing the transparency principle would reveal whether ICANN or its agents have violated other policies, such as:

- "[S]ustain[ing] … and promoting competition," *id.* Art. I §§ 5, 6;
- "Making decisions by applying documented policies neutrally and objectively, with integrity and fairness," *id.* Art. I § 8;
- "Remaining accountable to the Internet community," *id.* Art. I § 10; and

- Not "apply[ing] its standards, policies, procedures, or practices inequitably or singl[ing] out any particular party for disparate treatment," *id.* Art. II § 3.

Requestors urge the BGC to act to assure compliance with these critical policies by reconsidering ICANN's response to the RFP and directing that it produce all documents responsive to it.

4. Date of action:

ICANN's RFP response (the "Response") bears the date of 3 September 2014.

5. On what date did you become aware of the action?

The URL reflects posting of the Response on 4 September 2014 – https://www.icann.org/resources/pages/20140804-01-2014-09-04-en – and Requestors first became aware of it on that date.

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

6.1. Under the New gTLD Applicant Guidebook ("Guidebook" or "AGB"), "a qualified community application eliminates all directly contending standard applications, regardless of how well qualified the latter may be." AGB § 4.2.3 at 4-9. "Qualified" in this context means an application that attains community status as a result of CPE. *Id.* Because Hotel TLD prevailed in CPE, Requestors can no longer compete for the String.

6.2. The action of the CPE panel thus materially – indeed, terminally – affected Requestors. As such, they sought reconsideration of the CPE findings, contending that "the Panel has not followed the AGB policy and process for conducting CPE" as set forth in the Guidebook. https://www.icann.org/en/system/files/files/request-despegar-online-et-al-28jun14-en.pdf at 5-10.

6.3. Requestors also at that time claimed breach of other ICANN principles from the Bylaws and other governing documents, including ICANN's commitments to:

- "provide a … reasoned explanation of decisions,"

- make decisions "by applying documented policies neutrally and objectively," and
- "operate … in an open and transparent manner."

Id. at 10, *citing* ICANN's Affirmation of Commitments Art. 7 and Bylaws Arts. I § 2.8 and III § 1. The CPE process violated these tenets by (i) not making available the identities or qualifications of the panelists, (ii) not disclosing all materials considered by the panel, and (iii) not giving sufficient analysis and reasons for the panel's decision. *Id.* at 10-11.

6.4. The BGC construed Requestors' position in that prior matter as contesting the substance of the panel's determination, which it held insufficient for reconsideration. *See* https://www.icann.org/en/system/files/files/determination-despegar-online-et-al-22aug14-en.pdf at 7, 8, 9. It also ruled that the Guidebook does not require the panel to reveal the information that Requestors had sought, so that it did not violate any "established policy" of ICANN in not making such disclosures. *Id.* at 10-11.

6.5. Meanwhile, Requestors attempted to determine by their RFP whether the qualifications, selection, training and potential influence over the panel may have violated established ICANN policies pertaining, for example, to non-discrimination, neutrality, accountability and objective, fair application of documented policies. ICANN's refusal to provide the requested information obstructs Requestors' efforts to determine if it or the panel overstepped such policies, which would give them a basis for reconsideration or other review that this Tribunal previously had found lacking.

6.6. The overarching principle of transparency exists to ensure that ICANN and its agents comply with its other policies. Parties prevented from making such inquiries cannot enforce rights that they do not know they have or obtain remedies for violations they do not know have occurred. ICANN's sweeping rejection of the RFP has adversely affected Requestors in this material respect, entitling them to reconsideration here.

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

7.1. Without true transparency and accountability, the Internet community, for whose benefit ICANN operates,[1] can have no confidence that the organization with which it has entrusted the stewardship of the DNS in fact adheres to the principles upon which that trust rests. The DIDP process enables ICANN's multiple stakeholders to verify such compliance, and to correct transgressions and their consequences if and when they occur.

7.2. The underlying CPE determination has wiped out six capable competitors for a highly sought-after piece of Internet "real estate." Particularly when ICANN opens new swaths of the namespace, preferring a single party over another – or, as in this case, many others – not only restricts competition in that single instance, but also can discourage it in the future.

7.3. Also, a number of applicants have filed on a community basis and have gone through or await invitation to CPE. Similar results can occur and parties should have the ability – and ostensibly do, through DIDP – to discover whether the processes affecting them took place in accordance with ICANN's own foundational principles.

7.4. Nor does this concern stop with CPE or even the new gTLD program as a whole. It can arise in connection with any ICANN action or inaction that impacts any of its constituency. All such affected parties may suffer if lapses in transparency go unchecked. The potential for recurrence further supports reconsideration now.

8. Detail of Board or Staff Action – Required Information

Staff Action: Refusal to produce documents responsive to the RFP, which contravenes ICANN's transparency doctrine and may mask other potential policy violations. Pertinent facts and procedural history appear in the "Detailed Explanation"

[1] *See* ICANN Articles of Incorporation § 4.

portion of this section. The policy abuses constituting grounds for reconsideration are discussed at greater length in Section 10, *infra*.

Board action: Not applicable; Requestors do not seek reconsideration of any Board action of which they are aware.

Provide the Required Detailed Explanation here:

8.1. Requestors all submitted standard applications for the String, and Hotel TLD applied for it as an asserted community. https://gtldresult.icann.org/application-result/applicationstatus/viewstatus. Hotel TLD thereafter received and accepted an invitation to undergo CPE. http://newgtlds.icann.org/en/applicants/cpe#status.

8.2. According to the just-cited webpage, "application comments and letters of support or opposition must be submitted within 14 days of the CPE Invitation Date in order to be considered by the CPE Panel." *Id.* Opposing statements are published. *See* https://gtldcomment.icann.org/applicationcomment/viewcomments. Several Requestors, voicing concerns shared by all of them, filed oppositions to awarding Hotel TLD community priority.[2]

8.3. Hotel TLD posted a public response to the various opposition comments. https://gtldcomment.icann.org/applicationcomment/commentdetails/12399. Requestors do not know if Hotel TLD had any other communications, *ex parte* or otherwise, with ICANN, the CPE panel or anyone else involved in the CPE process.

8.4. Nor do Requestors have any information as to who served on the panel, what qualifications they had, how they got selected, and what communications they had internally or with ICANN, Hotel TLD or any other person concerning their evaluation. The panel issued its Report dated 11 June 2014, posted 12 June, finding that the Hotel TLD Application had satisfied the Guidebook-prescribed community criteria sufficiently

[2] *See*, *e.g.*, https://gtldcomment.icann.org/applicationcomment/commentdetails/12391; https://www.icann.org/en/system/files/correspondence/levy-to-willett-03mar14-en.pdf; https://www.icann.org/resources/correspondence/patetta-to-icann-2014-03-05-en.

to gain community priority. *See* **Annex A** hereto. This determination removed all of Requestors' applications from the .HOTEL contention set, AGB at 4-9, and left Hotel TLD a completely unencumbered path to delegation of the String.

8.5. As stated above, Requestors sought reconsideration of the Report as contrary to certain ICANN policies. The BGC did not agree, and denied the request. Links to the request and ruling, dated 28 June and 22 August 2014, respectively, appear in paragraphs 6.2 and 6.4, *supra*.

8.6. Requestors sent their 4 August 2014 RFP, **Annex B**, to didp@icann.org, the email address specified by ICANN for service of such requests. It sought documents identified verbatim as follows:

> 8.6.1. All correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication ("Communications") between individual member [sic] of ICANN's Board or any member of ICANN Staff and the Economist Intelligence Unit[3] or any other organization or third party involved in the selection or organisations of the CPE Panel for the Report, relating to the appointment of the Panel that produced the Report, and dated with the 12 month period preceding the date of the Report;
>
> 8.6.2. The curriculum vitaes ("CVs") of the members appointed to the CPE Panel;
>
> 8.6.3. All Communications (as defined above) between the CPE Panel and/or ICANN, directly related to the creation of the Report; and
>
> 8.6.4. All Communications (as defined above) between the CPE Panel and/or Hotel TLD or any other party prior with a material bearing on the creation of the Report.

[3] The EIU is the third party organization selected by and contracted with ICANN to evaluate all community-based applications invited to CPE.

Id. at 1. The RFP further outlined how the information requested above, defined as the "Requested Information" in the RFP,[4] "does not meet any of the defined conditions under the DIDP for non-disclosure …." *Id.* at 1-2.

8.7. ICANN's 3 September 2014 Response to the RFP, **Annex C**, posted on its website on 4 September, stated that ICANN did not have certain of the documents requested, yet admitted it had others but would not produce them due to claimed protections against disclosure specified in the DIDP. More specifically:

8.7.1. Claiming that, for the sake of "independence of the process and evaluation, ICANN … is not involved with the selection … of … individual evaluators" and does not have "information about who the evaluators on any individual panel may be," the Response represents that ICANN "does not have any CVs for the CPE Panel … [or] … regarding the appointment of the specific CPE Panel for the .HOTEL CPE," responsive to the requests reproduced above in paragraphs 8.6.1 and 8.6.2. App. C at 2. However, the Response *admits* that ICANN *does* have "documentation with the EIU for the performance of its role … as it relates to the .HOTEL CPE," but asserts that those documents satisfy "certain of the Defined Conditions of Nondisclosure set forth in the DIDP." *Id.*

8.7.2. Requestors do not agree with ICANN's asserted bars to disclosure. ICANN should not interpose such obstacles to access without providing a factual basis to determine if its claimed privileges have any merit. *At minimum*, the BGC should review the asserted protections and independently determine if they have any supportable grounds. Regardless, it should order production for the reasons set forth in Section 10 below.

8.7.3. With regard to the third item of the RFP, repeated at paragraph 8.6.3 above, ICANN represents that it "does not have any communications …

[4] Requestors define other capitalized herein, such as "Report" and "Hotel TLD," to have the same meanings as in the RFP.

with the evaluators that identify the scoring for any individual CPE …, [so] does not have documents of this type." Requestors do not dispute that ICANN cannot produce what it does not have. However, again, ICANN does concede that it has some documents responsive to this RFP – namely, "communications with persons from EIU who are not involved in the scoring of a CPE, but otherwise assist in a particular CPE …" Requestors should have access to such documentation, but ICANN again refuses to produce it on grounds *stated* in the DIDP but not *established* in the Response.

8.7.4. ICANN states that it also has documents responsive to the fourth category of the RFP, paragraph 8.6.4 above, constituting "Communications between the CPE Panel and Hotel TLD or any other party bearing on the creation of the Report." Specifically, while ICANN claims to have "limited the ability for requesters or other interested parties to initiate direct contact with the panels," it does concede that "the CPE Panel goes through a validation process regarding letters of support or opposition" as a matter of "direct communications," and that "from time to time ICANN is cc'd on the CPE Panel's verification emails." The Requestors properly seek those direct communications. The "verification process" could conclude that such communications are not appropriate, but could also reveal that the panel accepts certain communications that it should not. Even rejected communications, if reviewed, could potentially influence the panel or expose some policy violation.

As argued more fully below, transparency demands production of the Requested Information. Without it, ICANN has no accountability to its stakeholders or the public, and offers no assurance of compliance with its own policies on which its constituents rely in maintaining ICANN's role overseeing the DNS.

9. What are you asking ICANN to do now?

Applicant respectfully requests that the BGC:

9.1. Independently evaluate the legitimacy of ICANN's claimed grounds for withholding the Requested Information;

9.2. Regardless of whether certain protections against disclosure arguably exist, find that production of the Requested Information would serve policy interests that override any claimed basis for non-disclosure; and

9.3. Order ICANN to produce the Requested Information, subject to a protective order if the BGC deems it appropriate to facilitate production while preserving any potential confidentiality concerns.

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

10.1. Requestors have been adversely affected by the actions of ICANN staff in refusing to comply with the RFP. They have both procedural standing to make this Request and the substantive right to have it granted.

a) Requestors have standing to make this Request.

10.2. Requestors have been "adversely affected by ... one or more staff actions or inactions that contradict established ICANN policy …." This fact gives it standing within the meaning of Bylaws Art. IV § 2.2(a).

10.3. According to the form reconsideration request used here, a requestor must "demonstrate material harm and adverse impact" by the following measures:

10.3.1. *A loss or injury, financial or non-financial*. Requestors have described this in Section 6, *supra*. Namely, they have shown that ICANN's refusal to produce the Requested information has deprived them of the ability to determine if the underlying CPE process for the Application violated established ICANN policies that would provide a basis for challenging the process and either (i) redoing it with a properly constituted, trained, neutral and independent panel

free from undue influence, or (ii) reversing the result altogether as unsupported and resulting from improper conduct (if that is found to be the case).

10.3.2. *A direct and causal connection between the loss or injury and the staff action or inaction that is the basis of the Request*. Staff's rejection of the RFP has directly caused the injury. Without the Requested Information, Requestors cannot determine if they have a basis for review of the CPE under Article IV of the Bylaws.

10.3.3. *The relief requested must be capable of reversing the harm alleged*. Ordering disclosure directly reverses the harm stemming from nondisclosure.

By all measures, Requestors have standing to make this Request. They satisfy the procedural threshold of "material" and "adverse" impact in the form of specific injury, causation of that injury by ICANN staff action, and the ability of this proceeding to remedy that harm.

b) ICANN's obstinate Response to the RFP violates its own transparency policy and potentially conceals transgressions of other established policies.

10.4. As part of its "core values," ICANN provides for "[e]mploying open and transparent policy development mechanisms that … promote well-informed decisions based on expert advice …." Bylaws Art. I § 7. The Bylaws devote the entirety of their Article III to the subject of transparency.

10.5. As Article I, section 7 expressly acknowledges, transparency has as a key purpose the promotion of well-informed decisions. Requestors do not find the decision of the CPE panel in the underlying case well-informed, could only communicate their opposition to community priority in a public forum, and now know by ICANN's Response to the RFP that certain non-public communications did occur involving it, the EIU, the panel and other parties pertaining to the panel's role and its Report.

10.6. What do those communications show? Only ICANN and the other parties to them know. Requestors certainly do not. Nor does the public, which needs ICANN to act transparently to assure itself that ICANN is faithfully discharging its duties to:

- Promote competition, Bylaws Art. I §§ 2.5, 2.6;
- Apply polices documented in the AGB for the introduction of new TLDs and the determination of community priority neutrally, objectively and fairly, *id*. §§ 2.7, 2.8, Articles § 3;
- Apply controlling standards equitably, without singling out anyone for disparate and adverse treatment, Bylaws Art. II § 3;
- Act without bias, Bylaws Art. IV § 3.4.a, c; and
- Operate for the benefit of and remain accountable to the Internet community as a whole, Articles § 4, Bylaws Art. I § 10.

Transparency helps assure adherence as much as possible to all polices relevant to a particular situation, and the correction of lapses in such observances if and to the extent they occur.

10.7. Regardless of what the Requested Information may show, it should be disclosed. If it reveals anything from a "hiccup" to a "smoking gun," accountability dictates that Requestors have the opportunity to use that information to obtain whatever relief it may make available. If it establishes the Report and process leading up to it as "squeaky clean," transparency will have served the purpose of maintaining the parties' and others' confidence in ICANN and its systems.

10.8. Given the essential function of transparency and the many other policies implicated by it, this matter meets the substantive standards for reconsideration. The Response to the RFP as it stands now does not satisfy that threshold policy, making this Request proper and remedial action appropriate as set forth in Section 9 above.

11. Are you bringing this Reconsideration Request on behalf of multiple persons or entities? (Check one)

__X__ Yes

_____ No

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

Yes; all have lost the opportunity to compete for the String, and ICANN's withholding of information – which could reveal a policy violation giving them a basis for review of the CPE determination – harms them all equally.

Terms and Conditions for Submission of Reconsideration Requests

The Board Governance Committee has the ability to consolidate the consideration of Reconsideration Requests if the issues stated within are sufficiently similar.

The Board Governance Committee may dismiss Reconsideration Requests that are querulous or vexatious.

Hearings are not required in the Reconsideration Process, however Requestors may request a hearing. The BGC retains the absolute discretion to determine whether a hearing is appropriate, and to call people before it for a hearing.

The BGC may take a decision on reconsideration of requests relating to staff action/inaction without reference to the full ICANN Board. Whether recommendations will issue to the ICANN Board is within the discretion of the BGC.

The ICANN Board of Director's decision on the BGC's reconsideration recommendation is final and not subject to a reconsideration request.

DATED: September 19, 2014

Respectfully submitted,

THE IP and TECHNOLOGY LEGAL GROUP
dba New gTLD Disputes

By:___/jmg/_____
John M. Genga
Attorneys for Requestors

Documents Attached

Annex A: 11 June 2014 CPE Report re .HOTEL

Annex B: 4 August 2014 DIDP Request to ICANN

Annex C: 3 September 2014 ICANN Response to DIDP Request

crowell moring

Annex 14.

DETERMINATION
OF THE BOARD GOVERNANCE COMMITTEE (BGC)
RECONSIDERATION REQUEST 14-39

11 OCTOBER 2014

The Requesters—Despegar Online SRL; Radix FZC; Famous Four Media Limited; Fegistry, LLC; Donuts Inc.; and Minds + Machines—seek reconsideration of ICANN staff's response to the Requesters' request for documents pursuant to ICANN's Document Information Disclosure Policy ("DIDP"). The Requesters sought documents relating to a Community Priority Evaluation Panel's Report finding that HOTEL Top-Level Domain S.à.r.l.'s community application for the New gTLD .HOTEL prevailed in Community Priority Evaluation.

I. Brief Summary.

The Requesters each applied for .HOTEL. Hotel Top-Level-Domain S.à.r.l. ("Applicant") filed a community application for .HOTEL. Because the Applicant participated and prevailed in Community Priority Evaluation ("CPE"), none of the Requesters' applications for .HOTEL will proceed.

The Requesters subsequently filed a request pursuant to ICANN's DIDP ("DIDP Request"), seeking documents relating to the CPE Panel's Report finding that the Applicant had prevailed in CPE. In its response to the DIDP Request ("DIDP Response"), ICANN identified and provided links to all publicly available documents responsive to the DIDP Request and further noted that many of the requested documents did not exist or were not in ICANN's possession. With respect to those requested documents that were in ICANN's possession and not already publicly available, ICANN explained that those documents were not produced

because they were subject to certain of the Defined Conditions of Nondisclosure ("Nondisclosure Conditions") set forth in the DIDP.

On 22 September 2014, the Requesters filed Request 14-39, seeking reconsideration of ICANN's Response to the DIDP Request. The Requesters do not identify any policy or procedure that ICANN staff violated with respect to the DIDP Response, but simply disagree with ICANN staff's determination that certain requested documents were subject to one or more of the DIDP Nondisclosure Conditions and therefore not appropriate for public disclosure. Because the Requesters have failed to demonstrate that ICANN staff acted in contravention of established policy or procedure in responding to the DIDP Request, the BGC concludes that Request 14-39 be denied.

II. Facts.

A. Background Facts.

All six Requesters applied for .HOTEL.

The Applicant filed a community application for .HOTEL (*i.e.*, a seventh application for .HOTEL).

On 19 February 2014, the Applicant was invited to participate in the CPE process for HOTEL. The Applicant elected to participate in the process, and its .HOTEL community application ("Application") was forwarded to the CPE Panel ("Panel") assembled by the Economist Intelligence Unit ("EIU").

On 11 June 2014, the Panel issued its Report. The Panel determined that the Application sufficiently met the requirements specified in the Applicant Guidebook to achieve the necessary scores to prevail in CPE. Because the Application prevailed in CPE, none of the Requesters' applications in the .HOTEL contention set will proceed. (*See* Guidebook, § 4.2.3.)

On 28 June 2014, the Requesters filed Request 14-34, seeking reconsideration of the Panel's determination that the Application prevailed in CPE.

On 4 August 2014, the Requesters filed their DIDP Request, seeking:

1. All correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication ("Communications") between individual member[s] of ICANN's Board or any member[s] of ICANN Staff and the Economist Intelligence Unit or any other organisation or third party involved in the selection or organisation of the CPE Panel for the Report, relating to the appointment of the Panel that produced the Report, and dated within the 12 month period preceding the date of the Report;

2. The curriculum vitas ("CVs") of the members appointed to the CPE Panel;

3. All Communications (as defined above) between individual members of the CPE Panel and/or ICANN, directly relating to the creation of the Report; and

4. All Communications (as defined above) between the CPE Panel and/or Hotel TLD or any other party prior with a material bearing on the creation of the Report.

(*See* DIDP Request, Pgs. 1-2, *available at* https://www.icann.org/en/system/files/files/request-donuts-et-al-04aug14-en.pdf.)

On 22 August 2014, the BGC denied Request 14-34, determining that the Requesters "d[id] not identify any misapplication of a policy or procedure [with respect to the Report], but instead challenge[d] the merits of the Panel's Report, which is not a basis for reconsideration." (14-34 Determination, Pg. 1, *available at* https://www.icann.org/en/system/files/files/determination-despegar-online-et-al-22aug14-en.pdf.) The BGC also determined that "the Requesters' allusions to the broad fairness principles expressed in ICANN's Bylaws [could not] serve as a basis for reconsideration, as the Requesters d[id] not specify any specific Panel action that contravene[d] those principles." (*Id*., Pgs. 1-2.)

On 3 September 2014, ICANN responded to the Requesters' DIDP Request. (*See* DIDP Response, *available at* https://www.icann.org/en/system/files/files/response-donuts-et-al-03sep14-en.pdf.) ICANN identified and provided links to all publicly available documents

responsive to the DIDP Request. ICANN noted that many of the requested documents, such as "CVs for the CPE Panel," "documentation regarding the appointment of the specific CPE Panel for the .HOTEL CPE," and "communications . . . with the evaluators that identify the scoring for any individual CPE," did not exist or were not in ICANN's possession. (*Id*., Pg. 2.) With respect to those requested documents that were in ICANN's possession and were not already publicly available, ICANN explained that those documents would not be made publicly available because they were subject to certain DIDP Nondisclosure Conditions. (*Id*., Pgs. 2-3.)

On 22 September 2014, the Requesters filed Request 14-39, seeking reconsideration of the DIDP Response.

B. The Requester's Claims.

The Requesters contend that reconsideration is warranted because ICANN staff violated established policy and procedure by withholding from production certain documents determined to be subject to certain DIDP Nondisclosure Conditions. (Request, § 10, Pgs. 12-13.)

C. Relief Requested.

The Requesters ask the Board to: (i) "independently evaluate the legitimacy of ICANN's claimed grounds for withholding the Requested Information"; (ii) "[r]egardless of whether certain protections against disclosure arguably exist, find that production of the Requested Information would serve policy interests that override any claimed basis for non-disclosure"; and (iii) "[o]rder ICANN to produce the Requested Information, subject to a protective order if the BGC deems it appropriate." (Request, § 9, Pg. 11.)

III. Issues.

In view of the claims set forth in Request 14-39, the issues for reconsideration are whether ICANN staff violated established policy or procedure by declining to produce certain

documents sought through the DIDP Request and determined to be subject to certain DIDP Nondisclosure Conditions.

IV. The Relevant Standards for Evaluating Reconsideration Requests and the Documentary Information Disclosure Policy.

ICANN's Bylaws provide for reconsideration of a Board or staff action or inaction in accordance with specified criteria.[1] (Bylaws, Art. IV, § 2.) Dismissal of a request for reconsideration of staff action or inaction is appropriate if the BGC concludes, and the Board or the NGPC agrees to the extent that the BGC deems that further consideration by the Board or NGPC is necessary, that the requesting party does not have standing because the party failed to satisfy the reconsideration criteria set forth in the Bylaws.

ICANN considers the principle of transparency to be a fundamental safeguard in assuring that its bottom-up, multi-stakeholder operating model remains effective and that outcomes of its decision-making are in the public benefit and are derived in a manner accountable to all stakeholders. A principal element of ICANN's approach to transparency and information disclosure is the commitment to make publicly available on its website a comprehensive set of materials concerning ICANN's operational activities. In that regard, ICANN has identified many categories of documents that are made public as a matter of due course. (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.) In addition to ICANN's practice of making so many documents public as a matter of course, the DIDP allows community members to request that ICANN make public documentary information "concerning ICANN's operational

[1] Article IV, § 2.2 of ICANN's Bylaws states in relevant part that any entity may submit a request for reconsideration or review of an ICANN action or inaction to the extent that it has been adversely affected by:

(a) one or more staff actions or inactions that contradict established ICANN policy(ies); or

(b) one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act; or

(c) one or more actions or inactions of the ICANN Board that are taken as a result of the Board's reliance on false or inaccurate material information.

activities, and within ICANN's possession, custody, or control," that is not already publicly available. (*Id*.)

In responding to a request for documents submitted pursuant to ICANN's DIDP, ICANN adheres to the "Process For Responding To ICANN's Documentary Information Disclosure Policy (DIDP) Requests," which is available at https://www.icann.org/en/system/files/files/didp-response-process-29oct13-en.pdf. Following the collection of potentially responsive documents, the DIDP process provides that "[a] review is conducted as to whether any of the documents identified as responsive to the Request are subject to any of the [Nondisclosure Conditions] identified at http://www.icann.org/en/about/transparency/didp." (*Id*.)

Pursuant to the DIDP, ICANN reserves the right to withhold documents if they fall within any of the Nondisclosure Conditions, which include, among others: (i) "[i]nformation provided by or to a government or international organization . . . in the expectation that the information will be kept confidential and/or would or likely would materially prejudice ICANN's relationship with that party;" (ii) "[i]nternal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process […];" (iii) "[i]nformation exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates […];" and (iv) "[i]nformation subject to the attorney-client, attorney work product privilege, or any other applicable privilege." (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.) In addition, ICANN may refuse "[i]nformation requests: (i) which are not reasonable; (ii) which are excessive or overly burdensome; (iii) complying with which is not feasible; or (iv) [which] are made with an abusive or vexatious purpose or by a vexatious or querulous individual." (*See id*.)

The DIDP process also provides that "[t]o the extent that any responsive documents fall within any [Nondisclosure Conditions], a review is conducted as to whether, under the particular circumstances, the public interest in disclosing the documentary information outweighs the harm that may be caused by such disclosure." (*See* https://www.icann.org/en/system/files/files/didp-response-process-29oct13-en.pdf.) It is within ICANN's sole discretion to determine whether the public interest in the disclosure of responsive documents that fall within one of the Nondisclosure Conditions outweighs the harm that may be caused by such disclosure. (*Id*.) Finally, the DIDP does not require ICANN staff to "create or compile summaries of any documented information," including logs of documents withheld under one of the Nondisclosure Conditions. (*Id*.)

V. Analysis and Rationale

The Requesters disagree with ICANN staff's determination that certain requested documents were subject to DIDP Nondisclosure Conditions, as well ICANN's determination that, on balance, the potential harm from the release of the documents subject to the Nondisclosure Conditions outweigh the public interest in disclosure. (Request, § 8.7.2, Pg. 9 ("Requestors do not agree with ICANN's asserted bars to disclosure.").) The Requesters claims do not support reconsideration.

A. ICANN Staff Adhered To The DIDP Process In Finding Certain Requested Documents Subject To DIDP Nondisclosure Conditions.

The Requesters identify no policy or procedure that ICANN staff violated with respect to the DIDP Response. Instead, Requesters disagree with ICANN staff's application of the DIDP

Nondisclosure Conditions, and claim that ICANN, in declining to produce such documents, violated ICANN's core commitment to transparency. (Request, § 10, Pgs. 12-13.)[2]

Specifically, the Requesters object to ICANN's determination to withhold: (1) "documentation with the EIU for the performance of its role … as it relates to the .HOTEL CPE"; (2) "communications with persons from EIU who are not involved in the scoring of a CPE, but otherwise assist in a particular CPE […]"; and (3) certain emails sent to the CPE Panel for the purpose of validating letters of support or opposition to an application, on which ICANN from time to time is copied. (Request, § 8, Pgs. 9-10.) The Requesters state that as to those categories of documents, they "do not agree with ICANN's asserted bars to disclosure." (*Id*., § 8, Pg. 9.) The Requesters, however, fail to demonstrate that ICANN contravened the DIDP process.

The DIDP identifies a number of "conditions for the nondisclosure of information," such as documents containing "[i]nformation subject to the attorney-client [privilege], attorney work product privilege, or any other applicable privilege" and/or containing "[i]nternal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications." (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.) It is ICANN's responsibility to determine whether requested documents fall within those Nondisclosure Conditions. Specifically, pursuant to the DIDP process, "a review is conducted as to whether the documents identified as responsive to the Request are subject to any of the [Nondisclosure Conditions] identified at http://www.icann.org/en/about/transparency/didp." (*See* https://www.icann.org/en/system/files/files/didp-response-process-29oct13-en.pdf (Process For Responding To ICANN's Documentary Information Disclosure Policy (DIDP) Requests).)

[2] The Requesters do not challenge the DIDP Response insofar as it states that certain documents do not exist within ICANN's custody.

Specifically, pursuant to the DIDP process, "a review is conducted as to whether the documents identified as responsive to the Request are subject to any of the [Nondisclosure Conditions] identified at http://www.icann.org/en/about/transparency/didp." (*See* https://www.icann.org/en/system/files/files/didp-response-process-29oct13-en.pdf.)

Here, in finding that certain requested documents were subject to Nondisclosure Conditions, ICANN adhered to the DIDP process. Specifically, as to "documentation with the EIU for the performance of its role" and "communications with persons from EIU who are not involved in the scoring of a CPE," ICANN analyzed the Requesters' requests in view of the DIDP Nondisclosure Conditions. ICANN determined that the requested documents were subject to several Nondisclosure Conditions, including those covering "information exchanged, prepared for, or derived from the deliberative and decision-making processes" and "confidential business information and/or internal policies and procedures." (DIDP Response, Pg. 3.)[3] As to the validation emails, ICANN determined that those documents were subject to the Nondisclosure Condition covering "information exchanged, prepared for, or derived from the deliberative and decision-making processes." (*Id*.)

As ICANN noted in the DIDP Response, notwithstanding the fact that Requesters' "analysis in [their DIDP] Request concluded that no Conditions for Nondisclosure should apply, ICANN must independently undertake the analysis of each Condition as it applies to the documentation at issue, and make the final determination as to whether any Nondisclosure Conditions apply." (Response, Pg. 4.) In conformance with the publicly posted DIDP process (*see* https://www.icann.org/en/system/files/files/didp-response-process-29oct13-en.pdf), ICANN

[3] ICANN also noted that at least some of these documents were draft documents and explained that drafts not only fall within a Nondisclosure Condition but also are "not reliable sources of information regarding what actually occurred or standards that were actually applied." (DIDP Response, Pgs. 3-4.) In their DIDP Request, the Requesters acknowledged that there were not seeking disclosure of drafts. (DIDP Request, Pg. 2.)

undertook such analysis, as noted above, and articulated its conclusions in the DIDP Response. While the Requesters may not agree with ICANN's determination that certain Nondisclosure Conditions apply here, the Requesters identify no policy or procedure that ICANN staff violated in making its determination, and the Requesters' substantive disagreement with that determination is not a basis for reconsideration.

B. ICANN Staff Adhered To The DIDP Process In Determining That The Potential Harm Caused By Disclosure Outweighed the Public Interest In Disclosure.

The DIDP states that if documents have been identified within the Nondisclosure Conditions, they "may still be made public if ICANN determines, under the particular circumstances, that the public interest in disclosing the information outweighs the harm that may be caused by such disclosure." (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.) The Requesters appear to argue that the publication of the documents they wished for ICANN to have made public through the DIDP "would serve policy interests that override any claimed basis for nondisclosure." (Request, § 9, Pg. 11.) Here again, the Requesters' disagreement with the determination made by ICANN in responding to the DIDP Request does not serve as a basis for reconsideration.

The fact that the Requesters believe that in this case the public interest in disclosing information outweighs any harm that might be caused by such disclosure does not bind ICANN to accept the Requesters' analysis. Here, in accordance with the DIDP process, ICANN conducted a review of all responsive documents that fell within the Nondisclosure Conditions, and determined that the potential harm did outweigh the public interest in the disclosure of certain documents. (DIDP Response, Pg. 4.) Specifically, ICANN stated that "ICANN has determined that there are no particular circumstances for which the public interest in disclosing the information outweighs the harm that may be caused to ICANN, its contractual relationships

and its contractors' deliberative processes by the requested disclosure." (*Id*.) Indeed, as noted above, many of the items in the DIDP Request seek documents whose disclosure "would or would be likely to compromise the integrity of . . . [the] deliberative and decision-making process." (*Id*. at Pg. 2.) Again, the Requesters identify no policy or procedure that ICANN staff violated in making its determination, and the Requesters' substantive disagreement with that determination is not a basis for reconsideration.

Finally, the BGC notes that the Requesters refer to their DIDP Requests as "Requests for Production," which is terminology typically used in discovery requests in litigation and wholly inapplicable in the DIDP context. The use of that terminology reflects a misunderstanding of the purpose and intent of the DIDP. The DIDP is not a litigation tool, but rather "is intended to ensure that information contained in documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, is made available to the public unless there is a compelling reason for confidentiality." (*See* https://www.icann.org/resources/pages/didp-2012-02-25-en.) The suggestion that the BGC could or should require the use of a litigation tool such as a protective order "to facilitate production while preserving any confidentiality concerns" further illustrates the Requesters' misunderstanding of the DIDP. The DIDP is not about making pieces of information available to specific interested parties; it is about whether requested items of information are proper for public disclosure.

In this case, ICANN staff properly followed all policies and procedures with respect to the Requesters' DIDP Request—they assessed the request in accordance with the guidelines set forth in the DIDP and determined, pursuant to those guidelines, that certain categories of requested documents were not appropriate for disclosure.

VI. Determination.

Based on the foregoing, the BGC concludes that the Requesters have not stated proper grounds for reconsideration, and therefore denies Request 14-39. As there is no indication that ICANN violated any policy or procedure with respect to its response to the Requesters' DIDP Request, Request 14-39 should not proceed. If the Requesters believe they have somehow been treated unfairly in the process, the Requesters are free to ask the Ombudsman to review this matter.

The Bylaws provide that the BGC is authorized to make a final determination for all Reconsideration Requests brought regarding staff action or inaction and that no Board (or NGPC) consideration is required. (Bylaws, Art. IV, § 2.15.) As discussed above, Request 14-39 seeks reconsideration of a staff action or inaction. As such, after consideration of this Request, the BGC concludes that this determination is final and that no further consideration by the Board is warranted.

crowell moring

Annex 15.

Board Governance Committee (BGC) Meeting Minutes

11 Oct 2014

BGC Attendees: Cherine Chalaby, Chris Disspain, Mike Silber, Ram Mohan, Ray Plzak, and Bruce Tonkin – Chair

BGC Member Apologies: Olga Madruga-Forti

Other Board Member Attendees:Fadi Chehadé

Executive and Staff Attendees: John Jeffrey (General Counsel and Secretary), Megan Bishop (Board Support Coordinator), Vinciane Koenigsfeld (Board Support Content Manager), Michelle Bright (Board Support Manager), Samantha Eisner (Associate General Counsel), and Amy Stathos (Deputy General Counsel)

Invited Guests:Asha Hemrajani

The following is a summary of discussions, actions taken, and actions identified:

1. Minutes – The BGC approved the minutes from the meeting on 4 September 2014.

2. Committee Slating – The BGC discussed Committee slating and noted that the Board will discuss the proposed slate later in the week, and that the slate will be subject to Board approval on 16 October 2014.Specifically, the BGC discussed which Board members should serve as chair of certain committees.

3. Board Leadership Slating – The BGC discussed Board leadership slating and noted that the Board will discuss the proposed slate later in the week, and which will be subject to Board approval on 16 October 2014.

4. 2015 Nominating Committee Chair-Elect – The BGC chair reminded the committee that, on 9 September 2014, following a BGC recommendation, the Board approved Stéphane Van Gelder as the 2015 NomCom Chair.At that time, the BGC was still conducting interviews of a short list of candidates for the NomCom Chair-Elect. The Chair noted that the BGC has concluded its interviews of the candidates for the Chair-Elect position. The BGC approved a motion recommending a candidate to the Board for the Chair-Elect position for NomCom, which the Board will consider later today.

5. Reconsideration Request 14-38 – Staff briefed the BGC regarding ICANN's Business Constituency, the Registries Stakeholder Group, and the Non-Commercial Stakeholders Group's ("Requesters"') request seeking reconsideration of the ICANN staff's 14 August 2014 posting of a proposed process for developing enhancements to ICANN's accountability mechanisms ("Proposed Process").On 29 August 2014, the Requesters

filed Reconsideration Request 14-38 claiming that ICANN staff failed to allow for community participation and consider community input in the development of the Proposed Process.Subsequent to the submission of this Request, ICANN addressed the request for additional time for community input into the process design through further dialogue and through the opening of an additional 21-day public comment period.The BGC notes the importance of the issues raised by the Requesters and hopes that the constructive dialogue that has recently been initiated over those issues continues. After discussion and consideration of the Reconsideration Request, the BGC agreed to reach out to the Requesters to determine whether they prefer to withdraw the Request or proceed to disposition.

- Action: BGC Chair to reach out to the Requesters as to whether they would prefer to withdraw the Request or proceed to disposition.

6. Reconsideration Request 14-39 – Ram Mohan abstained from participation in this matter noting conflicts.Staff briefed the BGC regarding Despegar Online SRL, Radix FZC, Famous Four Media Limited, Fegistry LLC, Donuts Inc., and Minds + Machines' ("Requesters'") request for reconsideration of ICANN staff's response to the Requesters' request for documents pursuant to ICANN's Document Information Disclosure Policy ("DIDP").The Requesters each applied for .HOTEL.HOTEL Top-Level Domain S.à.r.l. ("Applicant") filed a community application for .HOTEL.Because the Applicant participated and prevailed in CPE, none of the Requesters' applications for .HOTEL will proceed.The Requesters subsequently filed a DIDP Request seeking documents relating to the CPE Panel's Report finding that the Applicant had prevailed in CPE.In its response to the DIDP Request, ICANN:(a) identified and provided links to all publicly available documents responsive to the DIDP Request; (b) noted that many of the requested documents did not exist or were not in ICANN's possession; and (c) explained that any remaining responsive documents were not produced because they were subject to certain of the Defined Conditions of Nondisclosure set forth in the DIDP.On 22 September 2014, the Requesters filed Request 14-39.The Requesters do not identify any policy or procedure that ICANN staff violated with respect to the DIDP Response, but simply disagree with the determination that certain requested documents were not appropriate for public disclosure. After discussion and consideration of the Request, the BGC concluded that the Requester has not demonstrated that ICANN staff acted in contravention of established policy or procedure in responding to the DIDP Request and, therefore, determined that Request 14-39 be denied.The Bylaws authorize the BGC to make a final determination on Reconsideration Requests brought regarding staff action or inaction and the BGC concluded that its determination on Request 14-39 is final; no consideration by the NGPC is warranted.

7. Guidance to Nominating Committee on Desired Board Member Skill Sets – The BGC reviewed the current draft of the Advice from the ICANN Board on Board Skills to the Nominating Committee (the "Advice").The Advice recommends that the NomCom use certain listed criteria as guidance when selecting Directors for the Board.After discussion and consideration of the Advice, the BGC agreed to send the the Advice to the NomCom.

- Action: Staff to send the Advice to the Nominating Committee.

Published on 23 October 2014