New gTLD Application Submitted to ICANN by: Booking.com B.V.

String: hotels

Originally Posted: 13 June 2012

Application ID: 1-1016-75482

Applicant Information

1. Full legal name

Booking.com B.V.

2. Address of the principal place of business

Herengracht 597
Amsterdam 1017 CE
NL

3. Phone number

+31 20 712 5600

4. Fax number

+31 20 7125609

5. If applicable, website or URL

http://www.booking.com

Primary Contact

6(a). Name

Mr. Winston Fuhriman

6(b). Title

Manager, Domain Services

6(c). Address

6(d). Phone Number

+1 208 685 1872

6(e). Fax Number

+1 208 389 5779

6(f). Email Address

tfuhriman3@markmonitor.com

Secondary Contact

7(a). Name

Mr. Rutger Prakke

7(b). Title

General Counsel

7(c). Address

7(d). Phone Number

+31 20 713 35 44

7(e). Fax Number

+31 20 715 31 51

7(f). Email Address

rutger.prakke@booking.com

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).

The Netherlands

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.

Priceline.com Bookings Acquisition Company 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

Darren Huston	Director
Glenn Fogel	Director
Olivier Bisserier	Director
Rutger Prakke	General Counsel

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

Darren Huston	Chief Executive Officer
Olivier Bisserier	Chief Financial Officer

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

Priceline.com Bookings Acquisition Company 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.

hotels

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.

As is the case with any new TLD that is added to the DNS root zone, some general technical acceptance issues with the delegation of this TLD are to be expected, which are entirely unrelated to the .hotels extension.
The Applicant has consulted various experts in the field of domain names, including – in particular – its selected back-end registry operator, who has a significant experience in introducing new TLDs to the DNS root, including .BIZ, .US, and .CO.

According to these parties, no particular issues with respect to this gTLD string are to be expected, since .hotels is a string that entirely consists of standard US ASCII characters, as is the case with most extensions currently available in the DNS. Furthermore, the length of the string is within the character restrictions that have been defined within the DNS.

Therefore, to the Applicant's best knowledge and belief, no specific issues are to be expected as regards the operation and rendering of the .hotels gTLD.

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.

Booking.com BV, a subsidiary of Priceline.com (Nasdaq:PCLN), is the No.1 online hotel reservations agency in the world, in terms of the number of online hotel room nights sold. Booking.com is dedicated to offering the best rates for all of the accommodation offered, attracting over 30 million unique visitors each month via the Internet from both leisure and business markets worldwide.

Established in 1996, Booking.com BV offers competitive rates for any type of property, ranging from small independent hotels to a five star luxury. The Booking.com website is available in 41 languages and offers more than 168,000 affiliated hotels in 160 countries around the world.

Booking.com B.V. is based in Amsterdam, the Netherlands, and is supported internationally by offices in: Amsterdam - Athens - Auckland - Bangkok - Barcelona - Berlin - Brussels - Buenos Aires - Cambridge - Cape Town - Casablanca - Chicago - Copenhagen - Dubai - Dublin - Edinburgh - Grand Rapids - Hong Kong - Honolulu - Houston - Innsbruck - Istanbul - Kuala Lumpur - Las Palmas de Gran Canaria - Las Vegas - Lille - Lisbon - London - Loulé (PT) - Lyon - Madrid - Málaga - Mexico City - Miami - Milano - Montréal - Moscow - Munich - New York - Nice - Norwalk - Orlando - Oslo - Paris - Prague - Riga - Rome - San Francisco - São Paulo - Shanghai - Singapore - Stockholm - Sydney - Tokyo - Vancouver - Venice - Vienna - Warsaw - Zagreb - Zürich.

Through its website, www.booking.com, Booking.com has built over the years an impressive brand, with a global exposure and a truly international clientele.

According to the Applicant, the purpose of the .hotels TLD may be manifold. A few of the main purposes currently intended are:

i. Pioneer the highly recognizable .hotels gTLD in order to further support its day-to-day activities, for the benefit of the Applicant, its affiliates, including hotels and hotel chains for which Booking.com provides hotel reservation services;

ii. Provide stakeholders of the Applicant, including subsidiaries, hotel partners, affiliate partners, users, and their respective directors, officers, employees, with a recognizable and trusted identifier on the Internet, creating additional level playing fields for the hotel industry under the authority of a prominent player in the hotel reservation marketplace. Such stakeholders may include, but are not limited to:

* its subsidiaries in various countries;
* business affiliates and partners, including individual hotels and hotel chains;
* prospective and current customers; and
* directors, officers and employees of the Applicant, its subsidiaries, hotel partners or business affiliates.

iii. Provide such stakeholders with a secure and safe Internet environment that is mainly or even fully under the control of the Applicant and its subcontractors;

iv. Providing customers of Booking.com and holders of domain name registrations in the .hotels gTLD with a service that aims at putting users first;

v. Offering multilingual hotel reservation services that are directly or indirectly accessible under specific domain names registered in the .hotels gTLD, referring to, amongst others, names of hotels, geographic locations in which affiliate hotels can be found, hotel categories, etc.

This just gives an idea of how Booking.com could use .hotels in the future. In the beginning, and until further developing a detailed plan to use this new gTLD, Booking.com’s intention is to implement a single registrant TLD.

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

Booking.com intends to organize the registry operation for the .hotels gTLD in such a manner that it will minimize the likelihood of having multiple applications or registration requests for a particular domain name.

According to the Applicant, Booking.com, this can be achieved in any of the following ways, which likely needs to be further refined following ICANN’s award and delegation of the .hotels gTLD to Booking.com:

i. From the Applicant’s perspective, .hotels may bring a high degree of recognition and specialization to the currently existing name space. Where in most cases the specific connotation that has been initially given to the gTLDs (or even ccTLDs) has disappeared, the .hotels top-level domain is currently intended to be unambiguous as regards:

* the identity of Booking.com as the Registry Operator;
* the source of the content and services offered under the .hotels gTLD, by Booking.com and⁄or a third party appointed by the latter;
* the affiliation between the Registry Operator and the .hotels gTLD, as well as the domain names registered in such gTLD; and
* in term, and at the discretion of Booking.com, the affiliation between the Registry Operator and any third party that may become authorized by Booking.com to register and⁄or use one or more domain name registrations in the .hotels gTLD, to be delegated and⁄or using such domain name registrations, providing content under such domain names and⁄or hotel reservations services.

ii. As mentioned in the vision and mission statement above, the key reasons why

Applicant is applying for .hotels include but are not limited to:

1. Operate the highly recognizable .hotels gTLD at the top-level of the DNS' hierarchy, for the benefit of the Applicant and the various stakeholders supported by the Applicant in its current day-to-day activities;

2. Safety and security; and

3. Implement measures – in the near or distant future and when more adequate tools and techniques become available – to mitigate and even avoid abuse, phishing, and even counterfeiting and piracy.

However, a further detailled plan on how the Applicant will use this gTLD has not been developed so far, which is mainly due to the short time frame between the announcement of the roll-out of the New gTLD Program, and the actual opening of the application window.

iii. The Applicant intends to implement the following policies and procedures with respect to the registration of domain names in the .hotels top-level domain:

(i) reservation and registration of domain names in the name of Booking.com. It is likely that this will be the scenario that Booking.com will put in place during the first months or even years of operation of the .hotels gTLD.

These names may include, but are not limited to:
a. descriptive names, referring to the actual day-to-day business activities of the Applicant or its Affiliates;
b. descriptive names, referring to the internal departments of the Applicant;
c. descriptive names, referring to the subsidiaries, affiliates and⁄or partners of the Applicant;
d. potentially also names relating to other stakeholders of Booking.com, to be determined by Booking.com following ICANN's award and delegation of the .hotels gTLD to Booking.com;
e. etc.

(ii) launch of the TLD: if and when implemented by the Registry Operator, this is likely going to be a gradual process, whereby selected third parties that meet certain criteria, which Booking.com will be entitled to set at its own discretion, may register domain names in the .hotels gTLD. These processes may include the following:

a. Sunrise: allow physical persons, organizations and entities that meet the eligibility requirements determined by Booking.com at that point in time to choose and, where allowed by Booking.com, to register the domain names that are identical to their trademarks. These parties are generally expected to include hotels and hotel chains, and the corresponding domain names would then include the names of hotels, hotel chains, including or excluding their geographic location;

b. Land rush and general availability: other available domain names may be registered by physical persons, organizations and entities that meet the eligibility requirements in force at that point in time to choose the domain names in accordance with the applicable terms and conditions.

Depending on the terms and conditions in force at the time of launch of the TLD, these domain names may or may not be registered in the name of the applicant for the domain name or in the name of the Registry Operator of the TLD (i.e., Booking.com). In any case, Booking.com reserves the right to impose additional and other restrictions from time to time at its sole discretion. These restrictions will be mainly inspired by the following elements and factors:

a. protecting and safeguarding the Applicant's brand and reputation;

b. the willingness to safeguard the trustworthiness of the .hotels gTLD, especially because of the fact that it will be operated by a respectable company;

c. the Applicants plan to provide users of the .hotels gTLD with a safe and secure experience; and

d. providing hotels and affiliates with a new indirect or – perhaps in the longer term – a more direct platform to promote themselves in the safe and secure .hotels online environment.

iv. Given the fact that the Applicant is a company that is established in the Netherlands, it is subject to both European and national privacy and data protection rules and practices. In particular, given the fact that the European and Dutch data protection authorities have issued strict guidelines, Booking.com will at all times be obliged to carefully consider and, where applicable, implement these policies, and this prior to and during the operation of the .hotels gTLD.

v. At this stage, Booking.com has not developed concrete and tangible plans in order to develop specific domain name registration activities in the .hotels gTLD apart from the activities described above. However, it is clear that the Applicant intends to operate the .hotels gTLD to the joint benefit of the Applicant, its affiliates, business partners and customers. In this respect, the Applicant has different ways in order to make existing and future customers, visitors and stakeholders aware of the (gradual) development of a new online environment under the .hotels TLD, including but not limited to:

a. Direct and indirect marketing and branding initiatives;
b. Internet advertising campaigns, including paid search, pay-per-click advertising, etc.;
c. Using its current on line presences, including various URLs under the Applicant's key Booking.com domain name, in order to drive Internet traffic towards domain name registrations in the .hotels gTLD, hereby promoting this new space, provide relevant content with respect to hotels and hotel reservations, and the opportunity to make such reservations by way of a secured platform;
d. Email marketing campaigns;
e. etc.

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

In line with Booking.com's mission and purpose for the .hotels gTLD, it is first and foremost important for Booking.com to be able to operate the .hotels name space in a stable, secure and responsible manner, putting the interests of users first. Therefore, Booking.com will, if and when awarded the .hotels TLD by ICANN, devise clear and detailed policies and procedures to that effect.

However, considering the fact that the actual award and delegation of the .hotels gTLD to Booking.com is subject to the successful evaluation of our application, we have not yet defined in detail:

* the types of domain names that will be registered;
* who will be entitled to select which domain names will be registered
* who will be entitled to register such domain names;
* who will be entitled to use such domain names, and;
* which types of use will be allowed or recommended.

As we believe that the development and implementation of one or more business cases could likely take a couple of months or even years, we have only focused on a number of high-level characteristics of our plans in relation to the operation of the .hotels gTLD, as described above.

By all means, it is in Booking.com's self-interest to, on the one hand, make the most of this initiative, promote its own business interests together with those of its key affiliates, business partners, hotels and hotel chains, whilst mitigating risks for the brands and brand reputation of such stakeholders and

reducing the (social) costs for others.

In this context, Booking.com will devise policies that encompass and comprise the following features:

At least during the initial months or even years following the delegation of the .hotels gTLD to Booking.com, this extension is likely going to be a so-called "single registrant TLD" as contemplated by ICANN in Article 4.5 of the template Registry Operator Agreement ("Transition of Registry upon Termination of Agreement"). For the avoidance of doubt, a "single registrant TLD" is a TLD where "(i) all domain name registrations in the TLD are registered to, and maintained by, Registry Operator for its own exclusive use, and (ii) Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator."

Therefore, parties who are not Booking.com or – insofar and to the extent Booking.com deems appropriate – an Affiliate within the meaning of the Registry Operator Agreement will not be entitled to register domain names in the .hotels gTLD.

Booking.com believes this to be in line with two of the main elements in its vision and mission statement, namely:

* Protecting and safeguarding the .hotels gTLD, by keeping full control over the entire operation of the .hotels registry and most if not all domain names registered therein; and

* Guaranteeing to Booking.com's key stakeholders who are interacting with Booking.com by using domain name registrations in .hotels that they are in fact interacting with the brand owner or its authorized Affiliates or business partners.

Consequently, there will be no (social) costs for non-eligible (third) parties, given the fact that they will be unable to register domain names in the .hotels gTLD in the first place.

However, even if only Booking.com will be entitled to register domain names, this does not exclude the hypothesis that disputes may arise with one or more third parties as regards domain names that are registered in the .hotels gTLD.

In order to avoid these risks, Booking.com intends to implement the following policies and processes:

First, the domain names to be registered by Booking.com could relate to the following:

* registered trademarks of Booking.com;
* names of affiliates and/or hotel partners of Booking.com;
* names of departments within Booking.com, and its subsidiaries;
* etc.

Furthermore, Booking.com envisages registering a fair number of generic words that are directly or indirectly related to the day-to-day business activities and operations of Booking.com and its Affiliates.

Prior to effectively registering such domain names in the .hotels gTLD, Booking.com will require its legal department to review the list of these domain names on a regular basis in order to satisfy itself that they will not infringe the rights of third parties.

In any case, Booking.com shall claim to have a legitimate interest in these domain names, as they are merely descriptive of the activities, products or services of Booking.com. So even if one or more of these domain names would be protected by a registered trademark, held by a third party, it is likely that a claim under the Uniform Dispute Resolution Policy or Uniform Rapid Suspension

policy will fail.

As regards the names referred to in Specification 5 to the template Registry Operator Agreement, Booking.com will follow the processes and procedures established by ICANN and the Governmental Advisory Committee.

If Booking.com would determine, at its sole discretion, that it will gradually allow certain categories of stakeholders to register domain names in the .hotels gTLD in their own name, Booking.com will devise policies to that effect.

However, Booking.com will at all times be entitled to restrict, limit or expand, among others:

* the category or categories of stakeholders who will be entitled to register one or more domain names in the .hotels gTLD, including their criteria for qualification;
* the choice of domain name(s) registered in the .hotels gTLD by and per such eligible stakeholder (category);
* the use made by an and per eligible stakeholder of a domain name registered in the .hotels gTLD;
* the transfer of domain names registered in .hotels;
* etc.

Booking.com shall reserve the right to subject the registration or use of a domain name to internal approval processes and procedures, at each and every step of the domain name life cycle.

Given the fact that Booking.com may release such available domain names post launch in a highly controlled manner, this also reduces the likelihood that two or more applicants qualify for the registration of the same domain name in the .hotels top-level domain;

As a method of last resort, and subject to the actual domain name registration policy adopted by the Registry Operator and in force at the time of registration, domain names will be allocated on a first-come, first-served basis.

In any event, Booking.com reserves the right to change or restrict any policies, procedures and practices at any point in time, especially if it is of the opinion that, e.g. there would be a risk that the reputation of the Booking.com brand or the brands of its stakeholders would be damaged.

It could be possible that the Applicant decides to make the .hotels top-level domain available to qualifying domain name registrants at an acceptable cost to them. Furthermore, Booking.com reserves the right to bundle certain products and services, such as hotel reservation and reservation modules with the registration of domain names in the .hotels gTLD. Furthermore, Booking.com may offer additional services that intend to drive Internet traffic from URLs operated by Booking.com towards domain names registered, controlled, and⁄or operated by such third parties.

So, in brief:

1. The Applicant ⁄ Registry Operator may reserve, delegate and use a potentially large number of domain names that are directly or indirectly relevant to Applicant’s business in its own name. Since some of these domain names could be of a descriptive nature, the chances for qualifying ⁄ eligible applicants ⁄ registrants to register such domain names after the launch will be limited;

2. The Registry Operator shall be entitled at all times to release available domain names post launch in a highly controlled manner, which also reduces the likelihood that two or more applicants qualify for the registration of the same domain name in the .hotels top-level domain;

3. As a method of last resort, and subject to the actual domain name registration policy adopted by the Registry Operator and in force at the time of registration, domain names will be allocated on a first-come, first-served basis, however

always taking into account the rights and legitimate interests of third parties, including but not limited to trademark rights;

4. The Applicant may make the .hotels top-level domain available to qualifying domain name registrants at an acceptable cost to them, to be determined if and when the Applicant would decide at its own discretion to allow third parties to register domain names, and – as the case may be – bundle such domain name registrations with additional added-value products and services generally offered by Booking.com in the course of its ordinary business activities, like operating the so-called "Bookit button", which is a tool that can be integrated in websites, and whereby customers can make direct hotel reservations through Booking.com's secure online transaction systems;

5. If the Applicant / Registry Operator will be required to increase the fees for the registration of domain names, such increases are intended to keep pace with comparable market rates for such domain name registrations. However, the Registry Operator shall at all times be entitled to bundle the registration of domain names with other products or services offered by or on behalf of Booking.com at a fee to be set by the Registry Operator.

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.

Given the fact that the Applicant is a hotel reservation agent, it has a vested interest in giving its visitors and clients a clear and predictable naming scheme in the .hotels gTLD. Since visitors and clients are mainly looking for hotel reservations on the basis of their geographic destination, the Applicant may indeed develop plans in order to register domain names that exclusively contain geographic names (country names, city names, names of regions, etc.).

However, if such domain names will be registered, the Applicant will do so considering the following confines:

(i) these domain names will be exclusively registered in the name of the Applicant / Registry Operator, and not in the name of a third party that is not controlled by the Applicant / Registry Operator, unless agreed upon otherwise with the authority competent for giving its consent in accordance with Specification 5 of the Registry Agreement;

(ii) where consents are required prior to the registration and use of a domain name referred to and in accordance with Specification 5 of the Registry Agreement, the Applicant will obtain such consents before actually registering, delegating and using these domain names.

In any case the registration, delegation and use of domain names corresponding to geographic names will at all times be done in the best interest of:

- the Applicant and its business as a hotel reservation agent; and

- in order to directly and indirectly promote hotel reservations, local tourism and business in the geographic locations of which the name has been registered in accordance with (i) above.

Registry Services

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

Response to Question 23 - Registry Services

23.1 Introduction

Booking.com has elected to partner with Neustar, Inc, to provide back-end services for the .hotels registry. In making this decision, Booking.com 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. These existing registry services will be leveraged for the .hotels 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. Booking.com will use Neustar's Registry Services platform to deploy the .hotels registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .hotels):

- 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.

23.2.1 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.

23.2.2 EPP

The .hotels 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.

23.2.3 DNS

Booking.com 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.

23.2.4 WHOIS

Neustar’s existing standard WHOIS solution will be used for the .hotels. The service provides support 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)

23.2.5 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.

23.2.6 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.

23.2.7 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.

23.2.8 Access to Bulk Zone Files

Booking.com 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.

23.2.9 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.

23.2.10 IPv6 Support

The .hotels 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.

23.2.11 Required Rights Protection Mechanisms

Booking.com, 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.

23.2.12 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

Booking.com will not be offering services that are unique to .hotels.

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

Response to Question 24 - Shared Registration System (SRS) Performance

24.1 Introduction

Booking.com has partnered with Neustar, Inc, an experienced TLD registry operator, for the operation of the .hotels 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

24.2.1 High-level SRS System Description

The SRS to be used for .hotels 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, Booking.com 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).

24.2.2 SRS Systems, Software, Hardware, and Interoperability

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

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

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

All interaction with the Registry is recorded in log files. Log files are generated at each layer of the system. These log files record at a minimum:

- The IP address of the client
- Timestamp
- Transaction Details
- Processing Time.

In addition to logging of each and every transaction with the SRS, Neustar maintains audit records, in the database, of all transformational transactions. These audit records allow the Registry, in support of the applicant, to produce a complete history of changes for any domain name.

24.2.3 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.

24.2.4 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.

24.2.5 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.

24.2.6 Database

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

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

24.2.7 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 .hotels 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.

24.2.8 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 .hotels.

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:

24.2.9 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.

24.2.10 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.

24.2.11 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.

24.2.12 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.

24.2.13 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.

24.2.14 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.

24.2.15 Compliance with Specification 6 Section 1.2

The SRS implementation for .hotels 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.

24.2.16 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 .hotels 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 .hotels 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 .hotels registry.

25. Extensible Provisioning Protocol (EPP)

Response to Question 25: Extensible Provisioning Protocol

25.1 Introduction

Booking.com's back-end registry operator, Neustar, Inc, 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 Booking.com is provided with an unparalleled EPP based registry. The following discussion explains the EPP interface which will be used for the .hotels 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.

25.3.1 EPP Toolkits

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

The software consists of working Java and C++ EPP common APIs and samples that implement the EPP core functions and EPP extensions used to communicate between the registry and registrar. The RTK illustrates how XML requests (registration events) can be assembled and forwarded to the registry for processing. The software provides the registrar with the basis for a reference implementation that conforms to the EPP registry-registrar protocol. The software component of the SDK also includes XML schema definition files for all Registry EPP objects and EPP object extensions. The RTK also includes a “dummy” server to aid in the testing of EPP clients.

The accompanying documentation describes the EPP software package hierarchy, the object data model, and the defined objects and methods (including calling parameter lists and expected response behavior). New versions of the RTK are made available from time to time to provide support for additional features as they become available and support for other platforms and languages.

25.4 Proprietary EPP Extensions

The .hotels 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 .hotels 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 .hotels registry is attached in the document titled "EPP Schema."

25.5 Resourcing Plans

The development and support of EPP is largely the responsibility of the Development/Engineering and Quality Assurance teams. As an experience registry operator with a fully developed EPP solution, on-going support is largely limited to periodic updates to the standard and the implementation of TLD specific extensions.

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

Development/Engineering – 19 employees
Quality Assurance - 7 employees.

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

26. Whois

Response to Question 26 – WHOIS

26.1 Introduction

Booking.com 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. Booking.com's back-end registry services provider, Neustar, Inc, 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 Neustar's solution that will be used in .hotels 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 .hotels thick-WHOIS solution also provides for additional search capabilities and mechanisms to mitigate potential forms of abuse as discussed below. (e.g., IDN, registrant data).

26.2 Software Components

The WHOIS architecture comprises the following components:

- An in-memory database local to each WHOIS node: To provide for the performance

needs, the WHOIS data is served from an in-memory database indexed by searchable keys.
- Redundant servers: To provide for redundancy, the WHOIS updates are propagated to a cluster of WHOIS servers that maintain an independent copy of the database.
- Attack resistant: To ensure that the WHOIS system cannot be abused using malicious queries or DOS attacks, the WHOIS server is only allowed to query the local database and rate limits on queries based on IPs and IP ranges can be readily applied.
- Accuracy auditor: To ensure the accuracy of the information served by the WHOIS servers, a daily audit is done between the SRS information and the WHOIS responses for the domain names which are updated during the last 24-hour period. Any discrepancies are resolved proactively.
- Modular design: The WHOIS system allows for filtering and translation of data elements between the SRS and the WHOIS database to allow for customizations.
- Scalable architecture: The WHOIS system is scalable and has a very small footprint. Depending on the query volume, the deployment size can grow and shrink quickly.
- Flexible: It is flexible enough to accommodate thin, thick, or modified thick models and can accommodate any future ICANN policy, such as different information display levels based on user categorization.
- SRS master database: The SRS database is the main persistent store of the Registry information. The Update Agent computes what WHOIS updates need to be pushed out. A publish-subscribe mechanism then takes these incremental updates and pushes to all the WHOIS slaves that answer queries.

26.3 Compliance with RFC and Specifications 4 and 10

Neustar has been running thick-WHOIS Services for over 10+ years in full compliance with RFC 3912 and with Specifications 4 and 10 of the Registry Agreement.RFC 3912 is a simple text based protocol over TCP that describes the interaction between the server and client on port 43. Neustar built a home-grown solution for this service. It processes millions of WHOIS queries per day.

Table 26-1 describes Neustar’s compliance with Specifications 4 and 10.

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

26.4 High-level WHOIS System Description

26.4.1 WHOIS Service (port 43)

The WHOIS service is responsible for handling port 43 queries. Our WHOIS is optimized for speed using an in-memory database and master-slave architecture between the SRS and WHOIS slaves.

The WHOIS service also has built-in support for IDN. If the domain name being queried is an IDN, the returned results include the language of the domain name, the domain name’s UTF-8 encoded representation along with the Unicode code page.

26.4.2 Web Page for WHOIS queries

In addition to the WHOIS Service on port 43, Neustar provides a web based WHOIS application (www.whois..hotels). It is an intuitive and easy to use application for the general public to use. WHOIS web application provides all of the features available in the port 43 WHOIS. This includes full and partial search on:

- Domain names
- Nameservers
- Registrant, Technical and Administrative Contacts

- Registrars

It also provides features not available on the port 43 service. These include:

1. Redemption Grace Period calculation: Based on the registry's policy, domains in pendingDelete can be restorable or scheduled for release depending on the date/time the domain went into pendingDelete. For these domains, the web based WHOIS displays "Restorable" or "Scheduled for Release" to clearly show this additional status to the user.
2. Extensive support for international domain names (IDN)
3. Ability to perform WHOIS lookups on the actual Unicode IDN
4. Display of the actual Unicode IDN in addition to the ACE-encoded name
5. A Unicode to Punycode and Punycode to Unicode translator
6. An extensive FAQ
7. A list of upcoming domain deletions

26.5 IT and Infrastructure Resources

As described above the WHOIS architecture uses a workflow that decouples the update process from the SRS. This ensures SRS performance is not adversely affected by the load requirements of dynamic updates. It is also decoupled from the WHOIS lookup agent to ensure the WHOIS service is always available and performing well for users. Each of Neustar's geographically diverse WHOIS sites use:

- Firewalls, to protect this sensitive data
- Dedicated servers for MQ Series, to ensure guaranteed delivery of WHOIS updates
- Packetshaper for source IP address-based bandwidth limiting
- Load balancers to distribute query load
- Multiple WHOIS servers for maximizing the performance of WHOIS service.

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

26.6 Interconnectivity with Other Registry System

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

26.7 Frequency of Synchronization between Servers

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

26.8 Provision for Searchable WHOIS Capabilities

Neustar will create a new web-based service to address the new search features based on requirements specified in Specification 4 Section 1.8. The application will enable users to search the WHOIS directory using any one or more of the following fields:

- Domain name

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

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

Figure 26-2 shows an architectural depiction of the new service.

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 .hotels 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 .hotels registry. The resources are more than adequate to support the WHOIS needs of all the TLDs operated by Neustar, including the .hotels registry.

27. Registration Life Cycle

Response to Question 27- Registration Life Cycle

27.1 Registration Life Cycle

27.1.1 Introduction

.hotels will follow the lifecycle and business rules found in the majority of gTLDs today. Booking.com's selected back-end operator for .hotels, Neustar, Inc, 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 .hotels.

27.1.2 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 .hotels registry per the defined .hotels 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 .hotels 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 .hotels 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 .hotels registry.
- Hold – Removes the domain from the DNS zone.
- UpdateProhibted – Prevents the object from being modified by an Update command.
- TransferProhibted – Prevents the object from being transferred to another Registrar by the Transfer command.
- RenewProhibted – Prevents a domain from being renewed by a Renew command.
- DeleteProhibted – 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.

27.2 Registration States

27.2.1 Domain Lifecycle – Registration States

As described above the .hotels 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.

27.2.2 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.

27.2.3 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.

27.2.4 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.

27.2.5 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.

27.2.6 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.

27.3 Typical Registration Lifecycle Activities

27.3.1 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.

27.3.2 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.

27.3.4 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.

27.3.5 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.

27.3.6 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.

27.4 Applicable Time Elements

The following section explains the time elements that are involved.

27.4.1 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.

27.4.2 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.

27.4.3 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).

27.4.4 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.

27.4.5 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.

27.4.6 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.

27.4.7 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.

27.5 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.

27.5.1 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.

27.6 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 .hotels 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 .hotels registry.

28. Abuse Prevention and Mitigation

Response to Question 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. Booking.com and its registry operator and back-end registry services provider, Neustar, Inc, 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 .hotels 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, Booking.com'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.

28.1.1 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 Booking.com's registry provider, Neustar is at the forefront of the prevention of such abusive practices and is one of the few currently existing registry operators to have actually developed and implemented an active "domain takedown" policy. Neustar also believes 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. Booking.com, through its registry provider Neustar, has an extensive, defined, and documented process for taking the necessary action of removing a domain from

the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the .hotels registry.

28.1.2 Abuse Point of Contact

As required by the Registry Agreement, .hotels 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. .hotels 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.

.hotels 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 of the Applicant 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 .hotels.

28.2.1 .hotels Acceptable Use Policy

This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any .hotels 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 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 .hotels'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 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. Registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

28.2.2 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 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 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.

28.2.2.1 Coordination with Law Enforcement

With the assistance of Neustar as its back-end registry services provider, Booking.com 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 .hotels 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 Booking.com 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".

28.3 Measures for Removal of Orphan Glue Records

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

While orphan glue often support correct and ordinary operation of the DNS, we understand that such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the 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 run 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 Booking.com or Neustar become 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.

28.4 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

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

29. Rights Protection Mechanisms

Response to Question 29 - Rights Protection Mechanisms

29.1. Rights Protection Mechanisms

Booking.com 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 for .hotels. Booking.com 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 Booking.com's selection of Neustar, Inc, as its registry services provider is Neustar's experience in successfully launching a number of TLDs with diverse rights protection mechanisms, including many the ones required in the Applicant Guidebook. More specifically, Booking.com will implement the following rights protection mechanisms in accordance with the Applicant Guidebook for .hotels 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 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 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

29.1.1 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, Booking.com 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, Booking.com'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 for .hotels.

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.

Booking.com'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 .hotels.

29.1.1.1 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 TLD 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 .hotels as required by ICANN.

a) 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
- 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 the registry. If they were not pre-validated, applicants were required to submit the required trademark information through their registrar to the Registry.

As the registry level, Neustar, subsequently either delivered the:

- Approval number and domain name registration information to the Clearinghouse
- 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 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 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, the application proceeded to registration when the .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 its 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.

b) Trademark Claims Service Experience

With Neustar's .biz TLD launched in 2001, Neustar became the first TLD with a Trademark Claims service. Neustar developed the Trademark Claim Service by enabling companies to stake claims to domain names prior to the commencement of live .biz domain registrations.

During the Trademark Claim 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.

29.1.2 Uniform Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension

(URS)

29.1.2.1 UDRP

Prior to joining Neustar, Mr. Jeff Neuman was 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 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 for which 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.

29.1.2.2 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) 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, it is the registry under the URS that must lock the domain within 24hours 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.

Booking.com is fully aware of each of these requirements and will have the capability to implement these requirements for new gTLDs in .hotels. 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 that it provides back-end registry services.

29.1.3 Implementation of Thick WHOIS

The .hotels 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.

29.1.4 Policies Handling Complaints Regarding Abuse

In addition the Rights Protection mechanisms addressed above, Booking.com will implement a number of measures to handle complaints regarding the abusive registration of domain names in its TLD as described in its response to Question 28.

29.1.4.1 Registry Acceptable Use Policy

One of the key policies each new gTLD registry is the 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. 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 name servers to collect information about the DNS queries to assist the investigation. .hotels'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.

29.1.4.2 Monitoring for Malicious Activity

Booking.com is committed to ensuring that those domain names associated with abuse or malicious conduct in violation of the Acceptable Use Policy for .hotels 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 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 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.

29.2 Safeguards against Unqualified Registrations

Pre-Authorization and Authentication

Prior to the release of any domain names, Applicant will designate that only designated employees will be authorized to register domain names within the TLD under strict domain name registration guidelines. Also, Applicant's registrar will verify the authenticity of the registrant. Additionally, prior to registration, registrar will validate contact information before the prospective registrant is allowed to proceed.

A variety of automated and manual procedures may be utilized for verification by the registrar as specified below:

- Applicant's registrar's automated authentication process will authenticate that the prospective registrant to verify authenticity;
- Applicant's registrar's will authenticate that the registrant's email is from Applicant based on a list of pre-approved email extensions from authorized related companies;
- If authenticated, the registrant will be allowed to submit and complete registrations;
- If the registrant cannot be verified by the registrar, the registrar will contact the registry to determine eligibility;
- Registrant must represent and warrant that neither the registration of the desired domain name, nor the manner in which the registration will be used, infringes the legal rights of third parties.

29.3 Resourcing Plans

The rights protection mechanisms described in the response above involve a wide range of Neustar 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- 4 employees
Customer Support – 12 employees

The resources are more than adequate to support the rights protection mechanisms of the .hotels registry.

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

Response to Question 30a - Security

30.(a).1 Security Policies

Booking.com and its back-end operator, Neustar, Inc, recognize the vital need to secure the systems and the integrity of the data in commercial solutions.
The .hotels 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 .hotels 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 .hotels
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 .hotels registry.

30.(a).2 Summary of Security Policies

Neustar 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).3 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).4 Augmented Security Levels and Capabilities

There are no increased security levels specific for .hotels. 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).5 Commitments and Security Levels

The .hotels 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